

#2
KWS
5-14-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Satoshi OBANA
Title: SIGNATURE CALCULATION
SYSTEM BY USE OF MOBILE
AGENT
Appl. No.: Unassigned
Filing Date: 1/17/2001
Examiner: Unassigned
Art Unit: Unassigned



CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japan Patent Application No. 2000-009037 filed 1/18/2000.

Respectfully submitted,

Date January 17, 2001

By Thomas J. Blumenthal Reg No 43,438

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

SATOSHI OBANA
72982/214

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 1月18日

出 願 番 号

Application Number:

特願2000-009037

出 願 人

Applicant(s):

日本電気株式会社

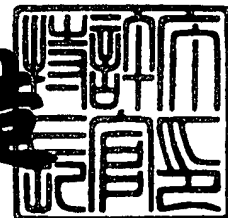


CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月13日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3084383

【書類名】 特許願

【整理番号】 33509672

【提出日】 平成12年 1月18日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00
H04L 9/32

【発明の名称】 移動エージェントによる署名計算システムおよびプログラムを記録した記録媒体

【請求項の数】 7

【発明者】
【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内
【氏名】 尾花 賢

【特許出願人】
【識別番号】 000004237
【氏名又は名称】 日本電気株式会社

【代理人】
【識別番号】 100108578
【弁理士】
【氏名又は名称】 高橋 詔男

【代理人】
【識別番号】 100064908
【弁理士】
【氏名又は名称】 志賀 正武

【選任した代理人】
【識別番号】 100101465
【弁理士】
【氏名又は名称】 青山 正和

【選任した代理人】
【識別番号】 100108453

【弁理士】

【氏名又は名称】 村山 靖彦

【手数料の表示】

【予納台帳番号】 008707

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9709418

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 移動エージェントによる署名計算システムおよびプログラムを記録した記録媒体

【特許請求の範囲】

【請求項1】 移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

乱数を出力する乱数生成手段と、

乱数生成手段から出力される乱数と移動エージェントの所有者の秘密鍵とを入力として、移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成手段と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段とを備えたベースホストを出発点として前記移動エージェントが移動を開始し、

移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化手段と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する移動エージェントの所有者の秘密鍵を用いたデジタル署名を計算することを特徴とする移動エージェントによる署名計算システム。

【請求項2】 移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

乱数を出力する乱数生成手段と、

乱数生成手段から出力される乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な補助データを

生成する部分署名補助データ生成手段と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段とを備えたベースホストを出発点として前記移動エージェントが移動を開始し、

移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成手段によって出力された前記新規秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化手段と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する前記新規秘密鍵を用いたデジタル署名を計算することを特徴とする移動エージェントによる署名計算システム。

【請求項3】 前記移動ホストにおける部分署名計算手段と部分署名署名化手段と公開鍵暗号計算手段とのうちの何れか一つ以上を移動エージェント側に設けたことを特徴とする請求項1または2記載の移動エージェントによる署名計算システム。

【請求項4】 移動エージェントがプログラムコードの実行を行うエージェント実行処理と、

乱数を出力する乱数生成処理と、

乱数生成処理で生成された乱数と移動エージェントの所有者の秘密鍵とを入力として、移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【請求項5】 移動エージェントがプログラムコードの実行を行うエージェ

ント実行処理と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化処理と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【請求項 6】 移動エージェントがプログラムコードの実行を行うエージェント実行処理と、

乱数を出力する乱数生成処理と、

乱数生成処理で生成された乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【請求項 7】 移動エージェントがプログラムコードの実行を行うエージェント実行処理と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成処理で生成された前記新規秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化処理と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ベースホストを出発した移動エージェントが移動先ホストにおいてデジタル署名を計算する場合に用いて好適な移動エージェントによる署名計算システムおよびベースホスト、移動ホストでそれぞれ用いられるプログラムを記録した記録媒体に関するものである。

【 0 0 0 2 】

【従来の技術】

移動エージェントは、移動エージェントの所有者の依頼した目的を達成するために、ネットワーク上に存在する複数のホストを自律的かつ動的に移動し、移動先のホストでプログラム・コードを起動し、処理していく。移動エージェントのセキュリティを保護する方式としては、移動エージェントのプログラム・コードの中に、公開鍵暗号や秘密鍵暗号のアルゴリズムを実装したプログラム・コードを格納して、悪意のある第三者によるデータの解析を困難にする方式や、移動エージェントのプログラム・コードに対して該移動エージェントの所有者の秘密鍵を用いて計算を行ったデジタル署名のデータをエージェントに保有させてネットワークを移動させる事によって、移動エージェントのプログラム・コードや保持するデータの改竄を困難にする方式が提案されている。

【 0 0 0 3 】

移動エージェントのセキュリティ保護に関する従来技術は、例えば特開平 1 0 - 2 6 9 1 8 6 号公報や特表平 1 1 - 5 0 6 2 2 2 号公報に詳しく述べられている。

【 0 0 0 4 】

【発明が解決しようとする課題】

上記特開平 1 0 - 2 6 9 1 8 6 号公報で述べられている技術では、悪意のある第三者がデータの解析や改竄を行う事を防止する事はできるが、移動先のホストに悪意がある場合には、移動先のホストによって移動エージェントの保有しているデータの解析が容易に行えるという問題がある。移動エージェントが移動先のホストでエージェントの所有者のデジタル署名を計算しようとする場合、エー

ジェントは該所有者の秘密鍵をエージェントに保有させる必要があるため、移動先のホストは、移動エージェントの保有するプログラム・コードおよびデータを解析する事により、該ユーザの秘密鍵を容易に知る事が可能であった。

【 0 0 0 5 】

この問題のため従来の技術では、移動エージェントが移動先のホストで該ホストが提示した任意のデータに対してデジタル署名を施す事は不可能であった。

【 0 0 0 6 】

また、特表平 1 1 - 5 0 6 2 2 2 号公報に述べられている技術では、署名計算を委託する移動ホスト等の機関が多数ある場合には、効率的の面で問題があった。尚、この公報の技術については、後述によりさらに説明する。

【 0 0 0 7 】

本発明の目的は、単独の移動先のホストでは解析できない形態で移動エージェント所有者の秘密鍵を移動エージェントに保有させる事により、移動先のホストに秘密鍵を知られる事なく、任意の移動先のホストが提示した任意の署名対象データに対する前記移動エージェント所有者のデジタル署名を計算し、前記署名対象データを提示した移動先のホストに渡す事にある。

【 0 0 0 8 】

また、本発明の他の目的は、単独の移動先のホストでは解析できない形態で移動エージェントの所有者にしか生成し得ない情報を移動エージェントに保有させる事により、任意の移動先のホストが提示した任意の署名対象データに対して前記情報を秘密鍵として用いたデジタル署名を計算し、前記署名対象データを提示した移動先のホストに渡す事にある。

【 0 0 0 9 】

【課題を解決するための手段】

上記の目的を達成するために、本発明による第 1 の移動エージェントによる署名計算システムは、移動エージェント（例えば第 1 の形態および第 1 の実施例における移動エージェント 1 4 0、5 4 0）がプログラムコードの実行を行うエージェント実行環境（同実行環境 1 0 5、5 0 5）と、乱数を出力する乱数生成手段（同乱数生成部 1 0 1、5 0 1）と、乱数生成手段から出力される乱数と移動

エージェントの所有者の秘密鍵（同秘密鍵 1 0 3、5 0 3）とを入力として、移動先のホスト（同移動先ホスト 1 1 0、1 2 0、1 3 0、5 1 0、5 2 0、5 3 0）で移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成手段（同部分署名補助データ生成部 1 0 4、5 0 4）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部 1 0 2、5 0 2）とを備えたベースホスト（同ベースホスト 1 0 0、5 0 0）を出発点として前記移動エージェントが移動を開始し、移動エージェントがプログラムコードの実行を行うエージェント実行環境（同実行環境 1 1 1、1 2 1、1 3 1、5 1 1、5 2 1、5 3 1）と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵（同秘密鍵 1 1 5、1 2 5、1 3 5、5 1 5、5 2 5、5 3 5）とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段（同部分署名計算部 1 1 2、1 2 2、1 3 2、5 1 2、5 2 2、5 3 2）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化手段（同部分署名署名化部 1 1 3、1 2 3、1 3 3、5 1 3、5 2 3、5 3 3）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部 1 1 4、1 2 4、1 3 4、5 1 4、5 2 4、5 3 4）とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する移動エージェントの所有者の秘密鍵を用いたデジタル署名を計算することを特徴とする。

【0 0 1 0】

また、本発明による第 2 の移動エージェントによる署名計算システムは、移動エージェント（例えば第 2 の形態および第 2 の実施例における移動エージェント 3 4 0、7 4 0）がプログラムコードの実行を行うエージェント実行環境（同実行環境 3 0 5、7 0 5）と、乱数を出力する乱数生成手段（同乱数生成部 3 0 1、7 0 1）と、乱数生成手段から出力される乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な

補助データを生成する部分署名補助データ生成手段（同部分署名補助データ生成部 3 0 4、7 0 4）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部 3 0 2、7 0 2）とを備えたベースホスト（同ベースホスト 3 0 0、7 0 0）を出発点として前記移動エージェントが移動を開始し、移動エージェントがプログラムコードの実行を行うエージェント実行環境（同実行環境 3 1 1、3 2 1、3 3 1、7 1 1、7 2 1、7 3 1）と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵（同秘密鍵 3 1 5、3 2 5、3 3 5、7 1 5、7 2 5、7 3 5）とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段（同部分署名署名化部 3 1 3、3 2 3、3 3 3、7 1 3、7 2 3、7 3 3）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成手段によって出力された前記新規秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化手段（同部分署名署名化部 3 1 3、3 2 3、3 3 3、7 1 3、7 2 3、7 3 3）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部 3 1 4、3 2 4、3 3 4、7 1 4、7 2 4、7 3 4）とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する前記新規秘密鍵を用いたデジタル署名を計算することを特徴とする。

【0011】

また、第 1、第 2 の移動エージェントによる署名計算システムにおいて、移動ホストを構成する部分署名計算手段、部分署名署名化手段および公開鍵暗号計算手段のうちの何れか一つ以上を削除するとともに、それを移動エージェント側に設けるようにしてもよい。

【0012】

また、本発明によるプログラムを記録した記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップ A 1、C 1）と、乱数を出力する乱数生成処理（例えばステップ A 2、C 2）と、乱数生成

処理で生成された乱数と移動エージェントの所有者の秘密鍵とを入力として、移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理（例えばステップ A 2, C 3）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理（例えばステップ A 2, C 4）とを実行するためのプログラムを記録したものである。

【 0 0 1 3 】

また、本発明による他のプログラムを記録した記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップ A 1 ～ A 6, A 1 0 ～ A 1 3, C 5 ～ C 8, C 1 9, C 2 3 ～ C 2 5）と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理（例えばステップ A 8, A 1 4, C 1 1 ～ C 1 7）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化処理（例えばステップ A 1 5, A 1 6, C 2 6 ～ C 2 8）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理（例えばステップ A 9, C 1 8 ～ C 2 2）とを実行するためのプログラムを記録したものである。

【 0 0 1 4 】

また、本発明による他のプログラムを記録した記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップ B 1 ～ B 7, B 1 2 ～ B 1 4, D 5 ～ D 8, D 1 9, D 2 3 ～ D 2 5）と、乱数を出力する乱数生成処理（例えばステップ B 2, D 2）と、乱数生成処理で生成された乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理（例えばステップ B 2, D 3）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理（例えばステップ B 2, D 4）とを実行するためのプログラムを記録したものである。

【 0 0 1 5 】

また、本発明による他の記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップB 1～B 7，B 1 1～B 1 4，D 5～D 8，D 1 9，D 2 3～D 2 5）と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理（例えばステップB 9，B 1 5，D 1 1～D 1 7）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成処理で生成された前記新規秘密鍵を用いて計算を行ったデジタル署名を出力する部分署名署名化処理（例えばステップB 1 6，B 1 7，D 2 6～D 2 8）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理（例えばステップB 1 0，D 1 8～D 2 2）とを実行するためのプログラムを記録したものである。

【 0 0 1 6 】

前記ベースホストにおいては、公開鍵暗号計算手段により秘密鍵を用いて公開鍵暗号によるデータの暗号化、復号およびデジタル署名の計算を行うとともに、部分署名補助データ生成手段により乱数と秘密鍵を用いて移動先ホスト i が移動エージェントのデジタル署名を計算するために必要なデータを計算することによって移動エージェントが移動先のホストで必要となるデータの準備を行う。移動先ホスト i ($1 \leq i \leq k$) においては、部分署名計算手段が、移動してきた移動エージェントが移動中にデジタル署名を付与する事を決定したメッセージと前記部分署名補助データ生成手段の出力とを入力として、移動エージェントの所有者のデジタル署名を計算するために必要なデータである部分署名の計算を行うとともに、部分署名署名化手段が一つまたは複数の移動先ホストによって計算された部分署名を入力として、前記のメッセージに対する移動エージェント所有者のデジタル署名を出力する。また、過去に移動エージェントが移動してきた際に計算した部分署名の出力結果や、移動先ホスト i が移動エージェントから削除した部分署名補助データを格納するとともに、公開鍵暗号計算手段は、移動先ホスト i ($1 \leq i \leq k$) によって計算された部分署名や部分署名補助データ計算手段の秘匿および改竄防止のために暗号化およびデジタル署名の付与を行う

ことにより、エージェントの依頼に応じて必要なデータの計算を行う。

【0017】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して詳細に説明する。

図1は、本発明の第1の実施形態による移動エージェントによる署名計算システムの構成を示すブロック図である。

本署名計算システムは、ベースホスト100と、移動先ホスト i ($1 \leq i \leq k$) と、移動エージェント140とを含んで構成される。図1では移動先ホスト i ($1 \leq i \leq k$) のうち、移動先ホスト1 (110) と移動先ホスト2 (120) と移動先ホスト k (130) が図示されている。また図中の黒く塗りつぶされた矢印は移動エージェント140の移動を表しており、また矢印が破線になっている部分は、その破線部分で複数のホストを移動していることを表している。

【0018】

次に、これらのホストと移動エージェントの概略的な構成及び動作について説明する。

ベースホスト100は、乱数生成部101と、公開鍵暗号計算部102と、移動エージェントの所有者の秘密鍵である秘密鍵0 (103) と、部分署名補助データ生成部104と、エージェント実行環境105とを含んで構成されている。

【0019】

乱数生成部101は部分署名補助データ生成部104の要求を受け、乱数を出力する。公開鍵暗号計算部102は、部分署名補助データ生成部104から受け渡されるデータを入力とし、この入力データの暗号化、復号、およびデジタル署名の計算を行う。デジタル署名を計算する際には、公開鍵暗号計算部102には移動エージェント140の所有者の秘密鍵である秘密鍵0 (103) も入力される。

【0020】

部分署名補助データ生成部104は、前記乱数生成部101の出力と移動エージェント140の所有者の秘密鍵である秘密鍵0 (103) とを入力とし、移動エージェント140が移動先ホスト i ($1 \leq i \leq k$) において、移動エージェン

ト 1 4 0 の所有者のデジタル署名を生成する際に必要なデータである部分署名を計算するための補助データを移動前の移動エージェント 1 4 0 内の中間データ格納部 1 4 1 に格納する。

エージェント実行環境 1 0 5 は、移動エージェント 1 4 0 がプログラム・コードの実行を行うための CPU 資源、メモリ等の計算環境を提供する。

【 0 0 2 1 】

移動先ホスト 1 (1 1 0) は、エージェント実行環境 1 1 1 と、部分署名計算部 1 1 2 と、部分署名署名化部 1 1 3 と、公開鍵暗号計算部 1 1 4 と、秘密鍵 1 (1 1 5) とデータ記憶部 1 1 6 とを含んで構成されている。

【 0 0 2 2 】

エージェント実行環境 1 1 1 は、前記エージェント実行環境 1 0 5 と同様に移動エージェント 1 4 0 がプログラム・コードの実行を行うための CPU 資源、メモリ等の計算環境を提供する。

【 0 0 2 3 】

部分署名計算部 1 1 2 は移動エージェント 1 4 0 が保持している部分署名補助データ生成部 1 0 4 の出力と移動エージェント 1 4 0 が複数の移動先ホストを移動している間に動的に決定された署名対象データと移動先ホスト 1 (1 1 0) の秘密鍵である秘密鍵 1 (1 1 5) とを入力として、移動エージェント 1 4 0 の所有者の秘密鍵である秘密鍵 0 (1 0 3) によるデジタル署名を計算するために必要なデータである部分署名を出力し、移動エージェント 1 4 0 内の中間データ格納部 1 4 1 に格納する。

【 0 0 2 4 】

部分署名署名化部 1 1 3 は、一つまたは複数の移動先ホスト i ($1 \leq i \leq k$) の部分署名計算部 1 1 2、1 2 2、1 3 2 によって出力され、移動エージェント 1 4 0 に格納された一つまたは複数の部分署名を入力として、移動エージェント 1 4 0 の所有者の秘密鍵である秘密鍵 0 (1 0 3) による前記署名対象データに対するデジタル署名を出力する。

【 0 0 2 5 】

公開鍵暗号計算部 1 1 4 は、前記部分署名計算部 1 1 2 の出力をデジタル署

名を渡すホスト以外に対して秘匿するために署名を渡すホストの公開鍵で該出力の暗号化を行う。また前記部分署名計算部 112 の出力を他の移動先ホストによって解析されたり改竄されることを防止するため、データを渡す相手の公開鍵による暗号化や移動ホスト 1 (110) の秘密鍵である秘密鍵 1 (115) を用いて前記部分署名計算部 112 の出力に対するデジタル署名の計算を行う。

【0026】

データ記憶部 116 は、移動エージェント 140 が再び同一のホストに移動するまでの間一時的に後に必要となるデータの格納を行う。

移動先ホスト i ($2 \leq i \leq k$) の構成については、移動先ホスト 1 (110) の構成と同様であるため詳細な説明は省略する。

【0027】

移動エージェント 140 は、中間データ格納部 141 を含んで構成されている。この中間データ格納部 141 は、ベースホスト 100 の部分署名補助データ生成部 104 および移動先ホスト i ($1 \leq i \leq k$) の部分署名計算部によって出力されるデジタル署名の計算に必要なデータの格納を行う。

【0028】

本実施形態では、移動エージェント 140 が複数の移動先ホストを移動後に到達した移動先ホスト 1 (110) が提示したデータに対する移動エージェント 140 の所有者のデジタル署名を、移動先ホスト i ($1 \leq i \leq k$) が計算するデータから生成を行う。

【0029】

次に図 1 および図 2 を参照して、本実施の形態による署名計算システムの全体の動作について詳細に説明する。

まず、署名を移動先のホストで計算する事を目的とした移動エージェント 140 がベースホスト 100 内のエージェント実行環境 105 で起動される (図 2 のステップ A1)。

【0030】

次に、部分署名補助データ生成部 104 が移動エージェント 140 の所有者の秘密鍵である秘密鍵 0 (103) と、乱数生成部 101 から出力される一つまた

は複数の乱数とを入力として、秘密鍵0（103）と予め定められた関係を満足する部分署名補助データを生成して出力し、移動エージェント140内の中間データ格納部141に格納する。後に移動エージェント140が移動した先のホストで、部分署名補助データが改竄されないために、出力された部分署名補助データは秘密鍵0によってデジタル署名が施され、部分署名補助データとともに中間データ格納部141に格納される（ステップA2）。

【0031】

移動エージェント140内の中間データ格納部141に部分署名補助データおよびデジタル署名が格納された後、移動エージェント140はネットワークを介して移動を開始する（ステップA3）。移動エージェント140は動的に0またはいくつかの移動先ホストを移動し、移動先のホストにデータを提示され、そのデータが署名を施す対象データであるかどうかの判断を行う（ステップA4）。

【0032】

0またはいくつかの移動先ホストを動的に訪問後、移動エージェント140の移動中に動的に決定された移動先ホスト1（110）に移動し（ステップA5、A6）、移動先ホスト1（110）からデータの提示を受ける。移動エージェント140は、移動先ホスト1（110）の提示したデータを署名対象データとして、移動エージェント140の所有者の秘密鍵である秘密鍵0（103）によるデジタル署名を計算する事を決定し、該署名対象データを移動エージェント140の中間データ格納部141に格納する（ステップA7）。

【0033】

署名対象データ決定後、移動先ホスト1（110）は中間データ格納部141に格納されているデータの全部または一部と、移動先ホスト1（110）の秘密鍵である秘密鍵1（115）とを部分署名計算部112に入力する事によって、移動エージェント140の所有者の秘密鍵0による署名対象データに対する署名を計算する際に必要となる部分署名を得る（ステップA8）。

【0034】

移動先ホスト1（110）は、部分署名計算部112に入力された中間データ

格納部 141 に格納されていたデータの中から以後に移動する移動先ホスト i ($2 \leq i \leq k$) で参照されないデータを中間データ格納部 141 から削除し、データ記憶部 116 に格納する。さらに部分署名計算部 112 の出力のうち以後に移動する移動先ホスト i ($1 \leq i \leq k$) で参照されないデータもデータ記憶部 116 に格納する。部分署名計算部 112 の出力のうち以後に移動する移動先ホスト i ($1 \leq i \leq k$) で参照されるデータは移動先ホスト 1 (110) の秘密鍵である秘密鍵 1 (115) によるデジタル署名を計算し、該署名とともに移動エージェント 140 内の中間データ格納部 141 に格納する (ステップ A9)。

【0035】

以上の処理が終了した後、移動エージェント 140 は次の移動先ホストである移動先ホスト 2 (120) に移動する (ステップ A10, A11, A12)。次に移動する移動先ホスト 2 (120) は、移動エージェント 141 が移動先ホスト 1 (110) に移動してきた時点で既に決定していたホストであっても、移動エージェント 141 が移動先ホスト 1 (110) に到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【0036】

以後に訪れる移動先ホスト i ($2 \leq i \leq k$) における処理の流れは i の値に関わらず同様であるため、代表して移動先ホスト i (120, 130) における処理の流れに関して説明する。

移動先ホスト i (120, 130) は移動エージェント 140 の中間データ格納部 141 に格納されているデータの全部または一部と、移動先ホスト i (120, 130) の秘密鍵である秘密鍵 i (125, 135) とを部分署名計算部 122, 132 に入力する事によって移動エージェント 140 の所有者の秘密鍵 0 による署名対象データに対する署名を計算する際に必要となる部分署名を得る。このとき部分署名計算部 122, 132 への入力となるデータに署名が付与されている場合には署名の検証を行う (ステップ A8)。

【0037】

移動先ホスト i (120, 130) は、部分署名計算部 122, 132 に入力された移動エージェント 140 の中間データ格納部 141 に格納されていたデー

タのうち、以後に移動する移動先ホスト j ($j = 1$ または $i + 1 \leq j \leq k$) で参照されないデータを公開鍵暗号計算部 124, 134 に入力する事によって、移動エージェントの所有者の公開鍵で暗号化を行い、得られた暗号文を中間データ格納部 141 に格納する。

【0038】

さらに部分署名計算部 122, 132 の出力のうち移動先ホスト j ($i + 1 \leq j \leq k$) で参照されないデータは公開鍵暗号計算部 124, 134 を用いて移動先ホスト 1 (110) の公開鍵で暗号化を行い、得られた暗号文を中間データ格納部 141 に格納する。部分署名計算部 122, 132 の出力のうち以後に移動する移動先ホスト j ($i + 1 \leq j \leq k$) で参照されるデータは移動先ホストの秘密鍵である秘密鍵 i (125, 135) によるデジタル署名を計算し、該署名とともに中間データ格納部 141 に格納する (ステップ A9)。

【0039】

以上の処理が終了した後、移動エージェント 140 は次の移動先ホストに移動する。次の移動先ホストは $i = k$ である場合には移動先ホスト 1 (110) となり、それ以外の場合には移動先ホスト $i + 1$ となる (ステップ A10, A11, A12, A13)。 $i \neq k$ の場合、次に移動する移動先ホスト $i + 1$ は、移動エージェント 141 が移動先ホスト i に移動してきた時点で既に決定していたホストであっても、移動エージェント 141 が移動先ホスト i に到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【0040】

移動エージェント 140 が再び移動先ホスト 1 (110) に移動した後、移動先ホスト 1 (110) は中間データ格納部 141 に格納されているデータの全部または一部と、移動先ホスト 1 (110) の秘密鍵である秘密鍵 1 (115) とを部分署名計算部 112 に入力する事によって、移動エージェント 140 の所有者の秘密鍵 0 による署名対象データに対するデジタル署名を計算する際に必要となる部分署名を得る (ステップ A14)。

【0041】

部分署名計算後、移動先ホスト 1 (110) は中間データ格納部 141 に格納

されているデータに対して該データが暗号化されている場合は、該データと移動先ホスト1の秘密鍵である秘密鍵1（115）を公開鍵暗号計算部114に入力する事によって該データの復号を行った後、復号したデータとデジタル署名を生成したホストの公開鍵を公開鍵暗号計算部114に入力する事によって該復号データに対する署名の検証を行い、該データが暗号化されていない場合は、該データとデジタル署名を生成したホストの公開鍵を公開鍵暗号計算部114に入力し、該データに対する署名の検証を行う事によってデータの改竄が行われていない事を確認する（ステップA15）。

【0042】

全てのデジタル署名の検証が終了した時点において、移動先ホスト1（110）は移動先ホスト i （ $1 \leq i \leq k$ ）によって計算された部分署名が得られる。移動先ホスト1（110）は得られた全てまたは一部の部分署名を部分署名署名化部113に入力する事によって、前記署名対象データに対して移動エージェントの所有者の秘密鍵である秘密鍵0によるデジタル署名が出力として得られる（ステップA16）。移動先ホスト1（110）は得られたデジタル署名をデータ記憶部116に格納し、移動エージェント140はベースホスト100に戻る（ステップA17）。

【0043】

次に、本実施の形態による効果について説明する。

以上の処理によって得られたデジタル署名は、移動エージェント140が移動したホストや移動した順序によらず、常に移動エージェントの所有者の公開鍵によって正当性が検証できるデジタル署名になっている。署名の偽造の可能性に関しては、移動エージェントの所有者の署名を生成するために、 k 個の移動先ホストの秘密鍵による演算が必要になるため、 k 個の移動先ホストが結託しない限りは署名の偽造を行う事を困難にすることができる。

【0044】

次に本発明の第2の実施の形態について説明する。

前述した第1の実施の形態では、移動エージェントが計算する署名が、移動先ホストが提示した署名対象データに対して移動エージェントの所有者の秘密鍵を

用いて計算した署名であったのに対し、本発明の第2の実施の形態では、移動エージェントが計算する署名が、移動エージェントのベースホストによって移動エージェントが移動を始める前に新規に生成された秘密鍵を用いて署名対象データに対して計算されたデジタル署名と、該ベースホストが新規に作成した秘密鍵に対応する公開鍵と、該公開鍵に対する移動エージェントの所有が予め所有している秘密鍵を用いて計算したデジタル署名のデータの三つ組みとなる点において異なっている。

【0045】

図3は、本発明の第2の実施形態による署名計算システムの構成を示すブロック図である。

本署名計算システムは、ベースホスト300と、移動先ホスト i ($1 \leq i \leq k$)と、移動エージェント340とを含んで構成される。図3では移動先ホスト i ($1 \leq i \leq k$)のうち、移動先ホスト1(310)と、移動先ホスト2(320)と、移動先ホスト k (330)が図示されている。また図中の黒く塗りつぶされた矢印は移動エージェント340の移動を表しており、また矢印が破線になっている部分は、その破線部分で複数のホストを移動していることを表している。

【0046】

次にこれらのホストと移動エージェントの構成および動作について概略的に説明する。

ベースホスト300は、乱数生成部301と、公開鍵暗号計算部302と、移動エージェント340の所有者の秘密鍵である秘密鍵0(303)と、部分署名補助データ生成部304と、エージェント実行環境305とを含んで構成されている。

上記構成要素のうち、乱数生成部301、公開鍵暗号計算部302、秘密鍵0(303)、エージェント実行環境305については、第1の実施形態における乱数生成部101、公開鍵暗号計算部102、秘密鍵0(103)、エージェント実行環境105とそれぞれ同一の動作であるため詳細な説明は省略する。

【0047】

部分署名補助データ生成部304は、前記乱数生成部301の出力を入力とし

、新規の秘密鍵と公開鍵の組の生成、移動エージェント 340 が移動先ホスト i ($1 \leq i \leq k$) において、前記の新規秘密鍵によるデジタル署名を生成するために必要となる部分署名を計算するための補助データを該データに対する移動エージェント 340 所有者の秘密鍵である秘密鍵 0 (303) によるデジタル署名とともに移動前の移動エージェント 340 内の中間データ格納部 341 へ格納する事、および前記の新規公開鍵を移動エージェント 340 所有者の秘密鍵である秘密鍵 0 (303) によるデジタル署名とともに移動前の移動エージェント 340 内の中間データ格納部 341 へ格納する事を行う。

【0048】

移動先ホスト 1 (310) は、エージェント実行環境 311 と、部分署名計算部 312 と部分署名署名化部 313 と公開鍵暗号計算部 314 とデータ記憶部 316 とを含んで構成されている。

上記構成要素のうち、エージェント実行環境 311、部分署名計算部 312、公開鍵暗号計算部 314、データ記憶部 316 については、第 1 の実施形態におけるエージェント実行環境 111、部分署名計算部 112、公開鍵暗号計算部 114、データ記憶部 116 とそれぞれ同一な動作であるため詳細な説明は省略する。

【0049】

部分署名署名化部 313 は一つまたは複数の移動先ホスト i ($1 \leq i \leq k$) の部分署名計算部 312、322、332 によって出力され、移動エージェント 340 に格納された一つまたは複数のデータを入力として、ベースホスト 300 の部分署名補助データ生成部 304 によって生成された新規秘密鍵によるデジタル署名と、中間データ格納部 341 に格納されている新規公開鍵と、該新規公開鍵に対する移動エージェント 340 所有者の秘密鍵である秘密鍵 0 (303) によるデジタル署名とを組にして移動エージェント 340 の所有者のデジタル署名として出力する。

移動先ホスト i ($2 \leq i \leq k$) および移動エージェント 340 の構成については、移動先ホスト 1 の構成と同じであるため詳細な説明は省略する。

【0050】

本実施形態では、移動エージェント340が複数の移動先ホストを移動後に到達した移動先ホスト1（310）が提示したデータに対する移動エージェント340の所有者のデジタル署名を、移動先ホスト i （ $1 \leq i \leq k$ ）が計算するデータから生成する。

【0051】

次に図3および図4を参照して本実施の形態による署名計算システムの全体の動作について詳細に説明する。

まず、署名を移動先のホストで計算する事を目的とした移動エージェント340がベースホスト300内のエージェント実行環境305で起動される（図4のステップB1）。

【0052】

次に、部分署名補助データ生成部304は乱数出力部301から出力される一つまたは複数の乱数を入力として新規に公開鍵と秘密鍵のペアを計算する。該公開鍵に対しては移動エージェント340の秘密鍵である秘密鍵0によるデジタル署名を計算し、署名とともに移動エージェント340内の中間データ格納部341に格納する（ステップB2）。

【0053】

次に部分署名補助データ生成部304は、乱数生成部301から出力される一つまたは複数の乱数とを入力として、ステップB2で生成した新規秘密鍵と予め定められた関係を満足する部分署名補助データを出力し、中間データ格納部341に格納する。後に移動エージェント340が移動した先のホストで部分署名補助データが改竄されないために、出力された部分署名補助データは秘密鍵0によるデジタル署名が施され、部分署名補助データとともに中間データ格納部341に格納される（ステップB3）。

【0054】

中間データ格納部341に部分署名補助データおよびデジタル署名が格納された後、移動エージェント340はネットワークを介して移動を開始する（図4のステップB4）。移動エージェント340は動的に0またはくつかの移動先ホストを移動し、移動先のホストにデータを提示され、そのデータが署名を施す対

象データであるかどうかの判断を行う（ステップB5）。

【0055】

0 またはいくつかの移動先ホストを動的に訪問後、移動エージェント340の移動中に動的に決定された移動先ホスト1（310）に移動し（ステップB6，B7）、移動先ホスト1（310）からデータの提示を受ける。移動エージェント340は、移動先ホスト1（310）の提示したデータを署名対象データとして、前記ベースホスト300の部分署名補助データ生成部304によって生成された新規秘密鍵によるデジタル署名を計算する事を決定し、該署名対象データを中間データ格納部341に格納する（ステップB8）。

【0056】

署名対象データ決定後、移動先ホスト1（310）は中間データ格納部341に格納されているデータの全部または一部と、移動先ホスト1（310）の秘密鍵である秘密鍵1（315）とを部分署名計算部312に入力する事によって前記ベースホスト300の部分署名補助データ生成部304によって生成された新規秘密鍵による署名対象データに対する署名を計算する際に必要となる部分署名を得る。このとき部分署名入力部322，332への入力となるデータに署名が付与されている場合には署名の検証を行う（ステップB9）。

【0057】

移動先ホスト1（310）は、部分署名計算部312に入力された中間データ格納部341に格納されていたデータの中から以後に移動する移動先ホスト i （ $2 \leq i \leq k$ ）で参照されないデータを該中間データ格納部341から削除し、データ記憶部316に格納する。さらに部分署名計算部312の出力のうち以後に移動する移動先ホスト i （ $1 \leq i \leq k$ ）で参照されないデータもデータ記憶部316に格納する。部分署名計算部312の出力のうち以後に移動する移動先ホスト i （ $1 \leq i \leq k$ ）で参照されるデータは移動先ホスト1（310）の秘密鍵である秘密鍵1（315）によるデジタル署名を計算し該署名とともに中間データ格納部341に格納する（ステップB10）。

【0058】

以上の処理が終了した後、移動エージェント340は次の移動先ホストである

移動先ホスト2 (320) に移動する (ステップB11, B12, B13)。次に移動する移動先ホスト2 (320) は、移動エージェント341が移動先ホスト1 (310) に移動してきた時点で既に決定していたホストであっても、移動エージェント341が移動先ホスト1 (310) に到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【0059】

以後に訪れる、移動先ホスト i ($2 \leq i \leq k$) における処理の流れは i の値に関わらず同様であるため、代表して移動先ホスト i (320, 330) における処理の流れに関して説明する。

移動先ホスト i (320, 330) は移動エージェント340の中間データ格納部341に格納されているデータの全部または一部と、移動先ホスト i (320, 330) の秘密鍵である秘密鍵 i 325, 335とを部分署名計算部322, 332に入力する事によって前記ベースホスト300の部分署名補助データ生成部304によって生成された新規秘密鍵による署名対象データに対するデジタル署名を計算する際に必要となる部分署名を得る (ステップB9)。

【0060】

移動先ホスト i (320, 330) は、部分署名計算部322, 332に入力された中間データ格納部341に格納されていたデータのち、以後に移動する移動先ホスト j ($j = 1$ または $i + 1 \leq j \leq k$) で参照されないデータを公開鍵暗号計算部324, 334に入力する事によって、移動エージェント340の所有者の公開鍵で暗号化を行い、得られた暗号文を中間データ格納部341に格納する。さらに部分署名計算部322, 332の出力のうち以後に移動する移動先ホスト j ($i + 1 \leq j \leq k$) で参照されないデータも公開鍵暗号計算部324, 334を用いて移動先ホスト1 (310) の公開鍵で暗号化を行い、暗号文を中間データ格納部341に格納する。

【0061】

部分署名計算部322, 332の出力のうち以後に移動する移動先ホスト j ($i + 1 \leq j \leq k$) で参照されるデータは移動先ホストの秘密鍵である秘密鍵 i 325, 335によってデジタル署名を計算し該署名とともに中間データ格納部

341に格納する（ステップB10）。

【0062】

以上の処理が終了した後、移動エージェント340は次の移動先ホストに移動する。次の移動先ホストは $i = k$ である場合には移動先ホスト1（310）となり、それ以外の場合には移動先ホスト $i + 1$ となる（ステップB11, B12, A13, B14）。 $i \neq k$ の場合、次に移動する移動先ホスト $i + 1$ は、移動エージェント340が移動先ホスト i に移動してきた時点で既に決定していたホストであっても、移動エージェント340が移動先ホスト i に到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【0063】

移動エージェント340が再び移動先ホスト1 310に移動した後、移動先ホスト1（310）は中間データ格納部341に格納されているデータの全部または一部と、移動先ホスト1（310）の秘密鍵である秘密鍵1（315）とを部分署名計算部312に入力する事によって前記ベースホスト300の部分署名補助データ生成部304によって生成された新規秘密鍵による署名対象データに対するデジタル署名を計算する際に必要となる部分署名を得る（ステップB15）。

【0064】

部分署名計算後、移動先ホスト1（310）は中間データ格納部341に格納されているデータに対して該データが暗号化されている場合は該データと移動先ホスト1（310）の秘密鍵である秘密鍵1（315）を公開鍵暗号計算部314に入力する事によって該データの復号を行った後、復号したデータとデジタル署名を生成したホストの公開鍵を公開鍵暗号計算部314に入力する事によって該復号データに対する署名の検証を行い、該データが暗号化されていない場合は該データと署名を生成したホストの公開鍵を公開鍵暗号計算部314に入力するし、該データに対する署名の検証を行う事によってデータの改竄が行われていない事を確認する（ステップB16）。

【0065】

全ての署名の検証が終了した時点において、移動先ホスト1（310）は移動

先ホスト i ($1 \leq i \leq k$) によって計算された部分署名が得られる。移動先ホスト 1 は得られた部分署名の全てまたは一部を部分署名署名化部 3 1 3 に入力する事によって、前記署名対象データに対して前記ベースホスト 3 0 0 の部分署名補助データ生成部 3 0 4 によって生成された新規秘密鍵によるデジタル署名が出力として得られる（ステップ B 1 7）。

【 0 0 6 6 】

移動先ホスト 1 (3 1 0) は得られたデジタル署名と、前記ベースホスト 3 0 0 の部分署名補助データ生成部 3 0 4 によって移動エージェント 3 4 0 内の中間データ格納部 3 4 1 に格納された新規公開鍵と該新規公開鍵に対する移動エージェント 3 4 0 の所有者の秘密鍵である秘密鍵 0 を用いて計算したデジタル署名をデータ記憶部 3 1 6 に格納し、移動エージェント 3 4 0 はベースホスト 3 0 0 に戻る（ステップ B 1 8）。

【 0 0 6 7 】

次に、本実施の形態による効果について説明する。

以上の処理によって得られたデジタル署名は、移動エージェントが移動したホストや移動した順序によらず、常に移動エージェントの所有者の公開鍵によって正当性が検証できる署名になっている。署名の偽造可能性に関しては、移動エージェントの所有者の署名を生成するために、 k 個の移動先ホストの秘密鍵による演算が必要になるため、 k 個の移動先ホストが結託しない限りは署名の偽造を行う事を困難にすることができる。更に k 個のホストが結託した場合でも、明らかになる情報はベースホストが新規に生成する秘密鍵だけであるので、ベースホストの所有者の秘密鍵は結託した悪意のある移動ホストに知られる事はない。

【 0 0 6 8 】

次に本発明の第 3 の実施の形態について説明する。

第 3 の実施の形態は、前述した第 1 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名計算部 1 1 2, 1 2 2, 1 3 2 が移動エージェント 1 4 0 のプログラム・コードによって実現されている点において異なる。

【 0 0 6 9 】

第3の実施の形態においては、移動エージェント140のプログラム・コードの入力として移動先ホスト i ($1 \leq i \leq k$)の秘密鍵が与えられるため、該秘密鍵を移動エージェント140の所有者および別の移動先ホストに知られないようにするために、移動エージェント140のプログラム・コードおよび中間データ格納手段に格納されている該秘密鍵の情報を移動エージェント140が次のホストに移動する前に消去する必要がある。

【0070】

次に本発明の第4の実施の形態について説明する。

第4の実施の形態は、第1の実施の形態において、移動先ホストに存在していた部分署名署名化部113, 123, 133が移動エージェント140のプログラム・コードによって実現されている点において異なる。

【0071】

次に本発明の第5の実施の形態について説明する。

第5の実施の形態は、第1の実施の形態において、移動先ホスト i ($1 \leq i \leq k$)に存在していた公開鍵暗号計算部114, 124, 134が移動エージェント140のプログラム・コードによって実現されている点において異なる。

【0072】

次に本発明の第6の実施の形態について説明する。

第6の実施の形態は、第1の実施の形態において、移動先ホスト i ($1 \leq i \leq k$)に存在していた部分署名計算部112, 122, 132および部分署名署名化部113, 123, 133が移動エージェント140のプログラム・コードによって実現されている点において異なる。

【0073】

次に本発明の第7の実施の形態について説明する。

第7の実施の形態は、第1の実施の形態において、移動先ホスト i ($1 \leq i \leq k$)に存在していた部分署名署名化部113, 123, 133および公開鍵暗号計算部114, 124, 134が移動エージェント140のプログラム・コードによって実現されている点において異なる。

【0074】

次に本発明の第 8 の実施の形態について説明する。

第 8 の実施の形態は、第 1 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名計算部 112, 122, 132 および公開鍵暗号計算部 114, 124, 134 が移動エージェント 140 のプログラム・コードによって実現されている点において異なる。

【0075】

次に本発明の第 9 の実施の形態について説明する。

第 9 の実施の形態は、第 1 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名計算部 112, 122, 132 および部分署名署名化部 113, 123, 133 および公開鍵暗号計算部 114, 124, 134 が移動エージェント 140 のプログラム・コードによって実現されている点において異なる。

【0076】

次に本発明の第 10 の実施の形態について説明する。

第 10 の実施の形態は、前述した第 2 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名計算部 112, 122, 132 が移動エージェント 140 のプログラム・コードによって実現されている点において異なる。

【0077】

上述した第 5 ～ 第 10 の実施の形態においては、移動エージェント 140 のプログラム・コードの入力として移動先ホスト i ($1 \leq i \leq k$) の秘密鍵が与えられるため、該秘密鍵を移動エージェント 140 の所有者および別の移動先ホストに知られないようにするために、移動エージェント 140 のプログラム・コードおよび中間データ格納手段に格納されている該秘密鍵の情報を移動エージェント 140 が次のホストに移動する前に消去する必要がある。

【0078】

次に本発明の第 11 の実施の形態について説明する。

第 11 の実施の形態は、第 2 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名署名化部 113, 123, 133 が移動エージェ

ント 1 4 0 のプログラム・コードによって実現されている点において異なる。

【 0 0 7 9 】

次に本発明の第 1 2 の実施の形態について説明する。

第 1 2 の実施の形態は、第 2 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた公開鍵暗号計算部 1 1 4, 1 2 4, 1 3 4 が移動エージェント 1 4 0 のプログラム・コードによって実現されている点において異なる。

【 0 0 8 0 】

次に本発明の第 1 3 の実施の形態について説明する。

第 1 3 の実施の形態は、第 2 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名計算部 1 1 2, 1 2 2, 1 3 2 および部分署名署名化部 1 1 3, 1 2 3, 1 3 3 が移動エージェント 1 4 0 のプログラム・コードによって実現されている点において異なる。

【 0 0 8 1 】

次に本発明の第 1 4 の実施の形態について説明する。

第 1 4 の実施の形態は、第 2 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名署名化部 1 1 3, 1 2 3, 1 3 3 および公開鍵暗号計算部 1 1 4, 1 2 4, 1 3 4 が移動エージェント 1 4 0 のプログラム・コードによって実現されている点において異なる。

【 0 0 8 2 】

次に本発明の第 1 5 の実施の形態について説明する。

第 1 5 の実施の形態は、第 2 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名計算部 1 1 2, 1 2 2, 1 3 2 および公開鍵暗号計算部 1 1 4, 1 2 4, 1 3 4 が移動エージェント 1 4 0 のプログラム・コードによって実現されている点において異なる。

【 0 0 8 3 】

次に本発明の第 1 6 の実施の形態について説明する。

第 1 6 の実施の形態は、第 2 の実施の形態において、移動先ホスト i ($1 \leq i \leq k$) に存在していた部分署名計算部 1 1 2, 1 2 2, 1 3 2 および部分署名署名化部 1 1 3, 1 2 3, 1 3 3 および公開鍵暗号計算部 1 1 4, 1 2 4, 1 3 4

が移動エージェント140のプログラム・コードによって実現されている点において異なる。

【0084】

本発明の第12～16の実施の形態においては、移動エージェント140のプログラム・コードの入力として移動先ホスト i ($1 \leq i \leq k$)の秘密鍵が与えられるため、該秘密鍵を移動エージェント140の所有者および別の移動先ホストに知られないようにするために、移動エージェント140のプログラム・コードおよび中間データ格納手段に格納されている該秘密鍵の情報を移動エージェント140が次のホストに移動する前に消去する必要がある。

【0085】

第3～16の実施の形態は、要するに第1、第2の実施の形態において、移動先ホストにおける部分署名部、部分署名署名化部、公開鍵暗号計算部のうちの何れか一つ以上を除くとともに、その除いたものを移動エージェント側に設けたものである。

【0086】

【実施例】

次に、本発明の具体的な実施例を図面を参照して説明する。

図5および図6は第1の実施例を示すブロック図である。

本実施例は、前述の第1の実施の形態による署名計算方式をRSA署名方式対応とするものである。

RSA署名方式は『「Handbook of Applied Cryptography」(A. Menezes, P. Oorschot, S. Vans tone著, CRC Press, 1997, ISBN 0-8493-8523-7) pp. 433-438』に詳しく述べられている。

【0087】

ここでは本実施例で用いる情報セキュリティの実現方式であるRSA署名方式, (k, n) 閾値秘密分散共有法, ElGamal暗号方式について簡単に説明する。

まずRSA署名方式について簡単に説明する。

RSA署名方式は512ビット程度の二つの素数 p, q の積 n と、 $\text{lcm}(p-1, q-1)$ (ここで $\text{lcm}(a, b)$ は a と b の最小公倍数を表すものとする)と互いに素である数 e との組 (n, e) を公開鍵として持ち、 $ed = 1 \pmod{\text{lcm}(p-1, q-1)}$ を満足する d を秘密鍵として持つ。

【0088】

M を署名を計算したいメッセージとすると、 M に対する署名 S は

$$S = M^d \pmod{n}$$

で表される。また、メッセージと署名のペア (M, S) を受信した受信者は、 (M, S) が式

$$M = S^e \pmod{n}$$

を満足する事を確かめる事により、メッセージの正当性を検証する。

【0089】

次に (k, n) 閾値秘密分散共有法について簡単に説明する。

(k, n) 閾値秘密分散法は秘密 S を次の(1), (2)の条件を満足するように n 人の参加者に秘密に関する分散情報を配布する方式である。

(1) k 人未満の参加者が集まって自分の保有する分散情報を公開しても秘密 S に関する情報は全く得られない。

(2) k 人以上の参加者が集まって自分の保有する分散情報を公開すると秘密 S は一意に復元される。

【0090】

(k, n) 閾値秘密分散共有法の実現方式に関しては『「Handbook of Applied Cryptography」(A. Menezes, P. Oorschot, S. Vanstone著, CRC Press, 1997, ISBN 0-8493-8523-7) pp. 525-526』に詳しく述べられている。

【0091】

ここでは多項式を用いた実現方式について簡単に説明する。

分散共有したい秘密 S ($1 \leq S < q$, q :素数)に対して、信頼できる第三者は以下のような多項式 $f(x)$ をランダムに選ぶ。

$$f(x) = S + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1} \pmod{q}$$

次に各参加者 i ($1 \leq i < n$) に分散情報として $v_i = f(i)$ を渡す。

【0092】

上述のように分散情報を定めると、上記 (1), (2) の性質がともに満たされる。 k 人の参加者 i_1, i_2, \dots, i_k が集まって自分の分散情報 $v_{i_1}, v_{i_2}, \dots, v_{i_k}$ を公開した場合、秘密 S は次式に従って復元される。

【0093】

【数1】

$$S = \sum_{j=1}^k L_{ij} v_{ij} \pmod{q}$$

【0094】

但し L_{ij} は次式で表される。

【0095】

【数2】

$$L_{ij} = \prod_{1 \leq j \leq k, i \neq j} \frac{i_i}{i_i - i_j} \pmod{q}$$

【0096】

次に ElGamal 暗号方式について説明する。

ElGamal 暗号方式は『「Handbook of Applied Cryptography」 (A. Menezes, P. Oorschot, S. Vanstone 著, CRC Press, 1997, ISBN 0-8493-8523-7) pp. 294-298』に詳しく述べられている。

【0097】

ここでは ElGamal 暗号方式の公開鍵、秘密鍵、暗号化法、復号法について簡単に説明する。

ElGamal 暗号方式は、512ビット程度の素数 p と、法 p の巡回群の生成元 g を共通パラメータとして持ち、秘密鍵 x ($0 \leq x < p$) を秘密鍵として持

ち、

$$y = g^x \pmod{p}$$

を公開鍵として持つ。

【0098】

mを暗号化したいメッセージとすると、送信者は乱数 r を選び、受信者の公開鍵 y を用いて $G = g^r$, $M = m y^r$ を計算し、(G, M) を暗号文として受信者に送る。暗号文 (G, M) を受信した受信者は、自分の秘密鍵 x を用いて $m = M / G^x$ を計算する事によりメッセージを復号する。

【0099】

本実施例では、移動エージェントの所有者は RSA 秘密鍵 d_A および対応する公開鍵 e_A を所有している。また移動先ホスト i ($1 \leq i \leq n$) も RSA 秘密鍵 d_i および対応する公開鍵 e_i を所有している。

【0100】

さらに本方式全体には k 個の El Gamal 暗号公開鍵 y_i ($1 \leq i < k$) が存在し、対応する秘密鍵 x_i ($1 \leq i < k$) は (i+1, n) 閾値秘密分散共有法を用いて各移動先ホスト j ($1 \leq j \leq n$) に秘密鍵として分散共有されている。以後、移動先ホスト j ($1 \leq j \leq n$) が保有する秘密鍵 x_i に対する分散情報を v_{ij} と表記する。このとき x_i を分散するのに用いた多項式 $f_i(x)$ に対して、

$$v_{ij} = f_i(1j)$$

が成立している。

【0101】

以上の準備の下、図5および図6を参照して本実施例の処理の流れについて説明する。

まずベースホスト500において移動エージェント540が起動される(図6のステップC1)。

【0102】

部分署名補助データ生成部504は秘密鍵 d_A と乱数生成手段501から出力される乱数を入力として

【0103】

【数3】

$$d_A = \sum_{i=1}^{k-1} r_i \pmod{\text{lcm}(p-1, q-1)}$$

【0104】

を満足する乱数 r_i ($1 \leq i < k$) を生成する (ステップ C 2)。得られた r_i

に対しては d_A による署名が計算され (ステップ C 3)、さらに E l G a m a l 暗号公開鍵 y_i を用いて暗号文 (G_i, M_i) が計算された後 (ステップ C 4)、暗号文 (G_i, M_i) および r_i に対する署名は移動エージェント 5 4 0 の中間データ格納部 5 4 1 に格納される。

【0105】

部分署名の計算に必要な補助データを中間データ格納部 5 4 1 に格納した後、移動エージェント 5 4 0 は移動を開始し (ステップ C 5)、いくつかの移動先ホストを動的に巡回した後 (ステップ C 6)、ホスト移動中に動的に決定された移動先ホスト 1 (5 1 0) に移動し (ステップ C 7, C 8)、移動先ホスト 1 (5 1 0) が提示したデータ m に対して署名を計算する事を決定する (ステップ C 9)。

【0106】

提示したデータ m に移動エージェント 5 4 0 が署名を計算する事を決定した後、移動先ホスト 1 (5 1 0) はステップ C 4 でベースホスト 5 0 0 によって計算され中間データ格納部 5 4 1 に格納されている暗号文 (G_i, M_i) ($1 \leq i < k$) を部分署名計算部 5 1 3 に入力する事によって G_{i1} を次式に従って計算する (ステップ C 1 0)。

【0107】

【数4】

$$G_{i1} = G_i^{V_{i1}} \pmod{p}$$

【0108】

G_{i1} ($1 \leq i < k$) を計算した後、更に移動先ホスト1 (510) は公開鍵暗号計算部514に、 G_{i1} と移動先ホスト1 (510) の秘密鍵 d_1 (515) を入力する事により、ステップC10で計算した G_{i1} に対する移動先ホスト1 (510) のRSAデジタル署名を計算する (ステップC11)。署名計算後、移動先ホスト1 (510) は G_{k-11} を移動先ホスト1 (510) のデータ記憶部516に格納し (ステップC12)、残りの計算結果 G_{i1} ($1 \leq i < k-1$) を移動エージェント540の中間データ格納部541に格納する (ステップC13)。中間データ格納部541にデータ格納をした後、移動エージェント540は次の移動先ホストである移動先ホスト2 (520) に移動する (ステップC14, C15)。

【0109】

移動エージェント540が移動先ホスト i ($2 \leq i \leq k$) に移動すると、移動先ホスト i はステップC4でベースホスト500によって計算され中間データ格納部541に格納されている暗号文(G_j, M_j) ($i-1 \leq j < k$) を部分署名計算部に入力する事によって G_{ji} を次式に従って計算する (ステップC16)。

【0110】

【数5】

$$G_{ji} = G_j^{V_{ji}} \pmod{p}$$

【0111】

G_{ji} ($i-1 \leq j < k$) を計算した後、移動先ホスト i は、計算した G_{ji} と移動先ホスト i の秘密鍵 d_i を公開鍵暗号計算部に入力する事によって G_j

i に対する移動先ホスト i の RSA 署名を計算し (ステップ C 17)、さらに G_{k-1i} を署名対象データの提示を行った移動先ホスト 1 (510) の公開鍵 e_1 で暗号化する (ステップ C 18)。ここで現在移動エージェント 540 が訪問している移動先ホストが移動先ホスト k (移動先ホスト 1 を訪問後 k 番目に訪問したホスト) であった場合には、移動エージェント 540 は移動先ホスト 1 に戻る (ステップ C 19, 25)。

【0112】

現在の移動先ホストが移動先ホスト k でない場合、この時点において、移動先ホスト i は G_{i-11} , G_{i-12} , G_{i-13} , ..., G_{i-1i} という i 個の G_{i-1j} ($1 \leq j \leq i$) なるデータを保有している。

【0113】

【数 6】

$$G_{i-1j} = G_{j-1}^{v_{i-1j}} \pmod{p}$$

【0114】

という関係と v_{i-1j} が (i, n) 閾値秘密分散共有法の部分情報である事に注意すると、

【0115】

【数 7】

$$\prod_{j=1}^i G_{i-1j}^{L_j} = G_{i-1}^{\sum_{j=1}^i L_j v_{i-1j}} = G_{i-1}^{x_{i-1}} \pmod{p}$$

【0116】

が成立する。ElGamal 暗号の復号法と比較すると、

【0117】

【数 8】

$$r_{i-1} = \frac{M_{i-1}}{\prod_{j=1}^i G_{i-1,j}^{L_j}} = \frac{M_{i-1}}{G_{i-1}^{x_{i-1}}} \pmod{p}$$

【0118】

が成立するので、部分署名計算部に $G_{i-1,1}$, $G_{i-1,2}$, $G_{i-1,3}$, ..., $G_{i-1,i}$ を入力して上記計算を行う事によって、 r_{i-1} が得られる。さらに部分署名部は m を入力として得る事により部分署名

【0119】

【数 9】

$$S_{i-1} = m^{r_{i-1}} \pmod{n}$$

【0120】

を出力する（ステップ C20）。

S_{i-1} が出力された後、移動先ホスト i は S_{i-1} と移動先ホスト 1 の公開鍵 e_1 とを公開鍵暗号計算部に入力して S_{i-1} を暗号化し、さらに S_{i-1} と移動エージェント 540 の所有者の公開鍵 d_i を公開鍵暗号計算部に入力して、 S_{i-1} に対する移動先ホスト i の RSA 署名を計算し、得られた暗号文および署名を移動エージェント 540 の中間データ格納部 541 に格納する（ステップ C21）。

【0121】

さらに以後の訪問先ホストで参照される事のないデータである $G_{i-1,j}$ ($1 \leq j \leq i$) と移動エージェント 540 の所有者の公開鍵 e_A を公開鍵暗号計算部に入力する事によって得られる $G_{i-1,j}$ に対する RSA 暗号文を中間データ格納部 541 に格納する（ステップ C22）。この暗号文データは、後にベースホスト 500 に戻った移動エージェント 540 が行ってきた計算を移動エージェント 540 の所有者が検証するために用いられる。

【0122】

移動先ホスト i によって計算されたデータが中間データ格納部 541 に格納された後、移動エージェント 540 は次の移動先である移動先ホスト $i+1$ に移動する（ステップ C23, 24）。この処理は図 6 においてステップ C16 に処理を戻す事に対応する。

【0123】

k 個の移動先ホスト、移動先ホスト 1 ～ 移動先ホスト k を訪問した移動エージェント 540 が移動先ホスト 1（510）に再び戻ってきた後、移動先ホスト 1（510）は公開鍵暗号計算部 514 を用いて、移動エージェント 540 の中間データ格納 541 に格納されている $e1$ を用いて暗号化されているデータの復号および検証可能である全ての署名の検証を行う（ステップ C26）。

【0124】

復号および署名検証が済んだ後、移動先ホスト 1 は G_{k-11} , G_{k-12} , …… G_{k-1k} という k 個の G_{k-1j} ($1 \leq j \leq k$) なるデータを保有している。ステップ C20 での操作と同様

【0125】

【数 10】

$$G_{k-1j} = G_{k-1}^{v_{k-1j}} \pmod{p}$$

【0126】

という関係と v_{k-1j} が (k, n) 閾値秘密分散共有法の部分情報である事に注意すると、

【0127】

【数 11】

$$\prod_{j=1}^k G_{k-1j}^{L_j} = G_{k-1}^{\sum_{j=1}^k L_j v_{k-1j}} = G_{k-1}^{x_{k-1}} \pmod{p}$$

【0128】

が成立するので、ElGamal 暗号の復号法と比較すると、

【0129】

【数 1 2】

$$r_{k-1} = \frac{M_{k-1}}{\prod_{j=1}^k G_{k-1,j}^{L_j}} = \frac{M_{k-1}}{G_{k-1}^{x_{k-1}}} \pmod{p}$$

【0 1 3 0】

が成立するので、部分署名計算部に $G_{k-1,1}$, $G_{k-1,2}$, ..., $G_{k-1,j}$ を入力する事によって、 r_{k-1} が得られる。さらに部分署名部は m を入力として得る事により部分署名

【0 1 3 1】

【数 1 3】

$$S_{k-1} = m^{r_{k-1}} \pmod{n}$$

【0 1 3 2】

を出力する（ステップ C 2 7）。

ステップ C 2 7 終了時に移動先ホスト 1 は k 個の部分署名 S_1 , S_2 , ..., S_k

を保有している。ここで各 S_i が

【0 1 3 3】

【数 1 4】

$$S_i = m^{r_i} \pmod{n}$$

【0 1 3 4】

という関係を満足する事と、

【0 1 3 5】

【数 1 5】

$$d_A = \sum_{i=1}^{k-1} r_i \pmod{\text{lcm}(p-1, q-1)}$$

【0136】

という関係が成立している事を考慮すると、部分署名署名化部が k 個の部分署名 S_i ($1 \leq i \leq k$) を入力とし、

【0137】

【数16】

$$\prod_{i=1}^{k-1} S_i = m^{\sum_{i=1}^{k-1} r_i} = m^{d_A} \pmod{n}$$

【0138】

を計算する事によって、移動先ホストが動的に提示した任意のデータ m に対して移動エージェント 540 の所有者の秘密鍵 d_A を用いて計算した RSA 署名が得られる。移動先ホスト 1 (510) は上記計算によって得られたデータを移動エージェント 540 による m に対する署名として格納する。署名を計算し終えた移動エージェント 540 はベースホスト 500 に戻る (ステップ C28)。

【0139】

次に、第2の実施例を図7および図8を参照して説明する。

本実施例は、前述の第2の実施の形態に係る署名計算方式を RSA 署名方式対応とするものである。

本実施例で用いる情報セキュリティの実現方式である RSA 署名方式、(k , n) 閾値秘密分散共有法、ElGamal 暗号方式については上述の第1の実施例と重複するため説明を省略する。

【0140】

本実施例では移動エージェントの所有者は RSA 秘密鍵 d_A および対応する公開鍵 e_A を所有している。また移動先ホスト i ($1 \leq i \leq n$) も RSA 秘密鍵 d_i および対応する公開鍵 e_i を所有している。

【0141】

さら本方式全体には k 個の ElGamal 暗号公開鍵 y_j ($1 \leq j < k$) が存在し、対応する秘密鍵 x_j ($1 \leq j < k$) は ($j+1$, n) 閾値秘密分散共有法を用いて各移動先ホスト i ($1 \leq i \leq n$) に秘密鍵として分散共有されてい

る。以後、移動先ホスト i ($1 \leq i \leq n$) が保有する秘密鍵 x_j に対する分散情報を v_{ij} と表記する。

【0142】

以上の準備の下、図7および図8を参照にして本実施例の処理の流れについて説明する。

まず図7のベースホスト700において移動エージェント740が起動される(図8のステップD1)。

【0143】

部分署名補助データ生成部704は乱数生成部701から出力される乱数を入力として新規のRSAの公開鍵(r_n, r_e), 秘密鍵 r_d および

$$r_d = \sum r_i \pmod{\text{lcm}(r_{p-1}, r_{q-1})}$$

を満足する乱数 r_i ($1 \leq i < k$) を生成する(ステップD2)。ここで、 r_p

, r_q は素数であり $r_n = r_p r_q$ を満足する。

【0144】

得られた新規公開鍵(r_n, r_e) および r_i に対しては d_A による署名が計算され(ステップD3)、さらにElGamal暗号公開鍵 y_i を用いて暗号文(G_i, M_i) が計算された後(ステップD4)、新規公開鍵(r_n, r_e), 新規公開鍵に対する署名 S_p , 暗号文(G_i, M_i) および r_i に対する署名は移動エージェント740の中間データ格納部741に格納される。

【0145】

部分署名の計算に必要な補助データを中間データ格納741に格納した後、移動エージェント740は移動を開始し(ステップD5)、いくつかの移動先ホストを動的に巡回した後(ステップD6)、ホスト移動中に動的に決定された移動先ホスト1(710)に移動し(ステップD7, D8) 移動先ホスト1(710) が提示したデータ m に対して署名を計算する事を決定する(ステップD9)。提示したデータ m に移動エージェント740が署名を計算する事を決定した後、移動先ホスト1(710) はステップD4でベースホストによって計算され中間

データ格納部741に格納されている暗号文(G_i, M_i) ($1 \leq i < k$)を部分署名計算部712に入力する事によって G_{i1} を次式に従って計算する(ステップD10)。

【0146】

【数17】

$$G_{i1} = G_i^{V_{i1}} \pmod{p}$$

【0147】

G_{i1} ($1 \leq i < k$)を計算した後、さらに移動先ホスト1(710)は公開鍵暗号計算部714に、 G_{i1} と移動先ホスト1の秘密鍵 d (715)を入力する事により、ステップD10で計算した G_{i1} に対する移動先ホスト1のRSAデジタル署名を計算する(ステップD11)。署名計算後、移動先ホスト1は G_{k-11} を移動先ホスト1(710)のデータ記憶部716に格納し(ステップD12)、残りの計算結果 G_{i1} ($1 \leq i < k-1$)を中間データ格納部741に格納する(ステップD13)。中間データ格納部741にヘデータ格納をした後、移動エージェント740は次の移動先ホストである移動先ホスト2(720)に移動する(ステップD14, D15)。

【0148】

移動エージェント740が移動先ホスト i ($2 \leq i \leq k$)に移動すると、移動先ホスト i はステップD4でベースホスト700によって計算され中間データ格納部741に格納されている暗号文(G_j, M_j) ($i-1 \leq j < k$)を部分署名計算部722に入力する事によって G_{ji} を次式に従って計算する(ステップD16)。

【0149】

【数18】

$$G_{ji} = G_j^{V_{ji}} \pmod{p}$$

【0150】

G_{ji} ($i-1 \leq j < k$)を計算した後、移動先ホスト i は、計算した G_{ji}

と移動先ホスト i の秘密鍵 d_i を公開鍵暗号計算部 724 に入力する事によって G_{ji} に対する移動先ホスト i の RSA 署名を計算し (ステップ D17)、さらに G_k

-1_j を署名対象データの提示を行った移動先ホスト 1 (710) の公開鍵 e_1 で暗号化する (ステップ D18)。ここで現在移動エージェント 740 が訪問している移動先ホストが移動先ホスト k (移動先ホスト 1 (710) を訪問後 k 番目に訪問したホスト) であった場合には、移動エージェントは移動先ホスト 1 (710) に戻る (ステップ D19, 25)。

【0151】

現在の移動先ホストが移動先ホスト k でない場合、この時点において、移動先ホスト i は G_{i-11} , G_{i-12} , ..., G_{i-1i} という i 個の G_{i-1j} ($1 \leq j \leq i$) なるデータを保有している。

【0152】

【数19】

$$G_{i-1j} = G_{i-1}^{v_{i-1j}} \pmod{p}$$

【0153】

という関係と v_{i-1j} が (i, n) 閾値秘密分散共有法の部分情報である事に注意すると、

【0154】

【数20】

$$\prod_{j=1}^i G_{i-1j}^{L_j} = G_{i-1}^{\sum_{j=1}^i L_j v_{i-1j}} = G_{i-1}^{x_{i-1}} \pmod{p}$$

【0155】

が成立する。ここで L_j は、前記の $v_{i-1j} = f_{i-1}(l_j)$ なる l_j を用いて次式で定義される。以後の L_j についても同様に定義されるものとする。

【0156】

【数 2 1】

$$L_j = \prod_{1 \leq j \leq m, m \neq j} \frac{l_m}{l_m - l_j} \pmod{q}$$

【0 1 5 7】

E l G a m a l 暗号の復号法と比較すると、

【0 1 5 8】

【数 2 2】

$$r_{i-1} = \frac{M_{i-1}}{\prod_{j=1}^i G_{i-1,j}^{L_j}} = \frac{M_{i-1}}{G_{i-1}^{x_{i-1}}} \pmod{p}$$

【0 1 5 9】

が成立するので、部分署名計算部に $G_{i-1,1}$, $G_{i-1,2}$, ..., $G_{i-1,i}$ を入力して上記計算を行う事によって、 r_{i-1} が得られる。さらに部分署名部は m を入力として得る事により部分署名

【0 1 6 0】

【数 2 3】

$$S_{i-1} = m^{r_{i-1}} \pmod{n}$$

【0 1 6 1】

を出力する（ステップ D 2 0）。

S_{i-1} が出力された後、移動先ホスト i は S_{i-1} と移動先ホスト 1（7 1 0）の公開鍵 e_1 とを公開鍵暗号計算部に入力して S_{i-1} を暗号化し、さらに S_{i-1} と移動エージェント 7 4 0 の所有者の公開鍵 d_i を公開鍵暗号計算部に入力し S_{i-1} に対する移動先ホスト i の RSA 署名を計算し、得られた暗号文および署名を中間データ格納部 7 4 1 に格納する（ステップ D 2 1）。

【0 1 6 2】

さらに以後の訪問先ホストで参照される事のないデータである G_{i-1j} ($1 \leq j \leq i$) と移動エージェント740の所有者の公開鍵 e_A を公開鍵暗号計算部に入力する事によって得られる G_{i-1j} に対するRSA暗号文を中間データ格納部741に格納する(ステップD22)。この暗号文データは、後にベースホスト700に戻った移動エージェント740が行ってきた計算を移動エージェント740の所有者が検証するために用いられる。

【0163】

移動先ホスト i によって計算されたデータが中間データ格納部741に格納された後、移動エージェント740は次の移動先である移動先ホスト $i+1$ に移動する(ステップD23, 24)。この処理は図8においてステップD16に処理を戻す事に対応する。

【0164】

k 個の移動先ホスト、移動先ホスト1～移動先ホスト k を訪問した移動エージェント740が移動先ホスト1(710)に再び戻ってきた後、移動先ホスト1(710)は公開鍵暗号計算部714を用いて、中間データ格納部741に格納されている e_1 を用いて暗号化されているデータの復号および検証可能である全ての署名の検証を行う(ステップD26)。

【0165】

復号および署名検証が済んだ後、移動先ホスト1(710)は G_{k-11} , G_{k-12} , ..., G_{k-1k} という k 個の G_{k-1j} ($1 \leq j \leq k$) なるデータを保有している。ステップD20での操作と同様

【0166】

【数24】

$$G_{k-1j} = G_{k-1}^{v_{k-1j}} \pmod{p}$$

【0167】

という関係と v_{k-1j} が (k, n) 閾値秘密分散共有法の部分情報である事に注意すると、

【0168】

【数25】

$$\prod_{j=1}^k G_{k-1j}^{L_j} = G_{k-1}^{\sum_{j=1}^k L_j v_{k-1j}} = G_{k-1}^{x_{k-1}} \pmod{p}$$

【0169】

が成立するので、ElGamal暗号の復号法と比較すると、

【0170】

【数26】

$$r_{k-1} = \frac{M_{k-1}}{\prod_{j=1}^k G_{k-1j}^{L_j}} = \frac{M_{k-1}}{G_{k-1}^{x_{k-1}}} \pmod{p}$$

【0171】

が成立するので、部分署名計算部に G_{k-11} , G_{k-12} , ..., G_{k-1i} を入力する事によって、 r_{k-1} が得られる。さらに部分署名部は m を入力として得る事により部分署名

【0172】

【数27】

$$S_{k-1} = m^{r_{k-1}} \pmod{n}$$

【0173】

を出力する（ステップD27）。

ステップD27終了時に移動先ホスト1（710）は k 個の部分署名 S_1 , S_2 , ..., S_k を保有している。ここで各 S_i が

【0174】

【数28】

$$S_i = m^{r_i} \pmod{n}$$

【0175】

という関係を満足する事と、

【0176】

【数29】

$$r_d = \sum_{i=1}^{k-1} r_i \pmod{\text{lcm}(r_p-1, r_q-1)}$$

【0177】

という関係（ここで r_p , r_q は $r_n = r_p r_q$ となる素数）が成立している事を考慮すると、部分署名署名化部が k 個の部分署名 S_i ($1 \leq i \leq k$) を入力とし、

【0178】

【数30】

$$\prod_{i=1}^{k-1} S_i = m^{\sum_{i=1}^{k-1} r_i} = m^{r_d} \pmod{r_n}$$

【0179】

を計算する事によって、移動先ホストが動的に提示した任意のデータ m に対して移動エージェント740のベースホスト700が新規に生成した秘密鍵 r_d を用いて計算したRSA署名 $S = m^{r_d}$ が得られる。

【0180】

移動先ホスト1（710）は上記計算によって得られた S と移動エージェントのベースホストによって新規に生成されたRSA公開鍵 (r_n, r_e) と、エージェント所有者の秘密鍵 d_A による (r_n, r_e) に対する署名 S_p の組 $(S, (r_n, r_e), S_p)$ を移動エージェント740による m に対する署名として格納する。署名を計算し終えた移動エージェント740はベースホスト700に戻る（ステップD28）。

【0181】

尚、各実施の形態および各実施例における移動エージェント、移動先ホストの

各コンピュータシステムにおいて、各フローチャートで説明した移動エージェントで実行される処理、および移動先ホストで実行される処理はコンピュータシステムにおけるROM等のメモリに格納されたプログラムに従って実行されるが、このメモリは本発明によるプログラムを記録した記録媒体を構成するものとなる。

このような記録媒体としては、各種のディスク媒体や半導体記憶装置、磁気記録媒体等を用いることができる。

【0182】

次に、前述した特表平11-506222公報に開示された技術と本発明とを比較検討する。

前記公報の請求項1～3は、「予め定められたエンティティ」の秘密鍵の情報を「予め定められた複数（定数： t 0 個）の機関」で分散管理し、分散情報を有する複数の機関が署名対象データに対して計算した部分署名を組み合わせることにより、正しいデジタル署名の計算を行う方式となっている。

【0183】

また前記公報の請求項4は、「あるエンティティ（不特定と解釈する事も可能）」の署名を計算する権限を「予め定められた複数（定数： t 0 個）の機関」に一時的に委託することを目的としており、「あるエンティティ」の秘密鍵の部分情報を予め定められた複数の機関に渡し、分散情報を有する複数の機関が署名対象データに対して計算した部分署名を組み合わせることにより、正しいデジタル署名の計算を行う方式となっている。

【0184】

これに対して本発明は、「不特定のエンティティ（本発明では移動エージェントの所有者）」の秘密鍵によるデジタル署名の計算を「不特定（エージェントが事前に知る事ができない）複数（定数）の機関（本発明では移動先ホスト）」に委託することを目的とし、不特定複数のどの移動先ホストが部分署名を計算した場合でも、正しいデジタル署名が計算されるという方式である（移動先ホストが移動エージェントが出発する前に部分署名を計算するホストを知る事ができない事は、前述により説明した通りである）。

【0185】

前記公報の請求項4を、その記載されている目的とは異なった使い方をする事によって、「不特定の複数の機関」に署名計算を委託する方式に転用する事は不可能ではないが（例えば署名計算を委託する可能性のある全ての機関から t_0 個を取り出す全ての可能な組み合わせに対して秘密鍵の部分情報を計算する等）、しかし、本発明が意図しているような署名計算を委託する可能性のある機関が膨大な数になるような場合には、効率の面から考えて大きなデメリットがあるものである。

【0186】

例えば、移動エージェントが移動のために携えていくデータサイズについて考えると、本発明では、 t_0 個に比例したサイズになるが、前記公報の技術では、署名計算を委託する可能性のあるホスト（個数 n ）を不特定にしようとした場合には、 $t_0 * n C t_0$ に比例したサイズになってしまう（ここで $a C b$ は、 a 個の中から b 個を取り出す可能な組み合わせの個数を表す）。

【0187】

以上述べたことから、

（1）本発明の方式は、部分署名の計算を行う機関が不特定である。即ち、前記公報の技術とは意図が異なる。

（2）仮に前記公報の方式を部分署名の計算を行う機関が不特定な場合に適用しようとしても、効率の面から問題があり、このような場合は、本発明を適用する方がメリットが大きいと言える。

【0188】

【発明の効果】

本発明の効果は、 k 個（ k ：定数）の移動先ホストが結託しない限り移動エージェントの所有者の秘密鍵によるデジタル署名を偽造が困難であるような形で移動エージェントにデータを持たせつつ、移動エージェントは移動先で提示される任意のデータに対して移動エージェントの所有者の秘密鍵を用いたデジタル署名を移動中に計算できることにある。

【0189】

その理由は、移動エージェントが署名を計算するためには、 k 個の移動先ホストによる部分署名が必要であり、部分署名の計算には移動先ホストの秘密鍵の情報が必要であるため、署名の偽造を行おうとした場合には、 k 個の秘密鍵を用いた演算が必要となるので、 k 個の移動先ホストが結託しない限りは署名の偽造が困難となるためである。

【図面の簡単な説明】

【図 1】 本発明の第 1 の実施の形態による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図 2】 第 1 の実施の形態の動作を示すフローチャートである。

【図 3】 本発明の第 2 の実施の形態による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図 4】 第 2 の実施の形態の動作を示すフローチャートである。

【図 5】 本発明の第 1 の実施例による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図 6】 第 1 の実施例の動作を示すフローチャートである。

【図 7】 本発明の第 2 の実施例による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図 8】 第 2 の実施例の動作を示すフローチャートである。

【符号の説明】

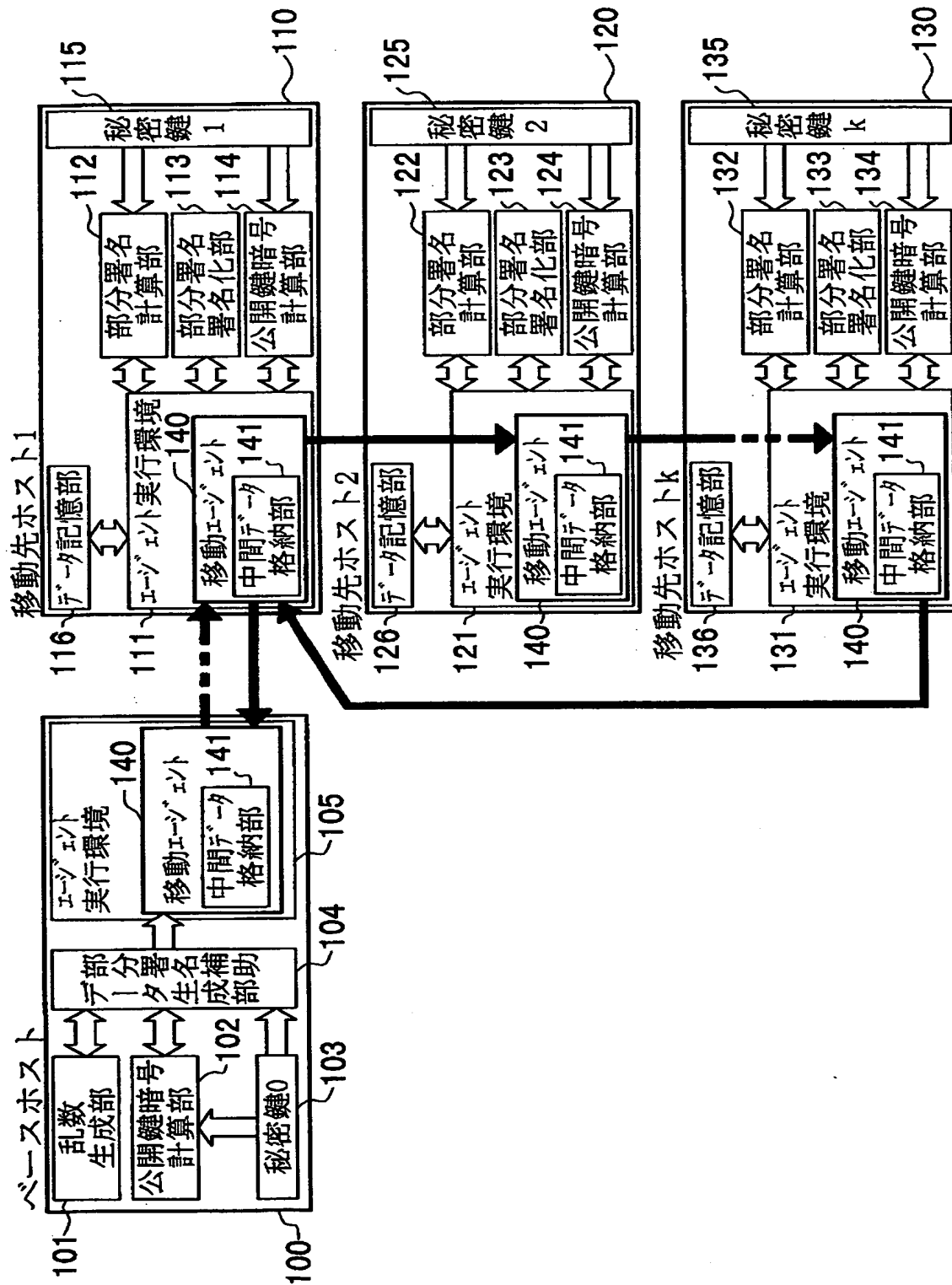
1 0 0, 3 0 0, 5 0 0, 7 0 0	ベースホスト
1 0 1, 3 0 1, 5 0 1, 7 0 1	乱数生成部
1 0 2, 3 0 2, 5 0 2, 7 0 2	公開鍵暗号計算部
1 0 3, 3 0 3, 5 0 3, 7 0 3	秘密鍵
1 0 4, 3 0 4, 5 0 4, 7 0 4	部分署名補助データ生成部
1 0 5, 3 0 5, 5 0 5, 7 0 5	エージェント実行環境
1 1 0, 3 1 0, 5 1 0, 7 1 0	移動先ホスト 1
1 2 0, 3 2 0, 5 2 0, 7 2 0	移動先ホスト 2
1 3 0, 3 3 0, 5 3 0, 7 3 0	移動先ホスト k
1 1 1, 1 2 1, 1 3 1,	

3 1 1, 3 2 1, 3 3 1,	
5 1 1, 5 2 1, 5 3 1,	
7 1 1, 7 2 1, 7 3 1	エージェント実行環境
1 1 2, 1 2 2, 1 3 2,	
3 1 2, 3 2 2, 3 3 2,	
5 1 2, 5 2 2, 5 3 2,	
7 1 2, 7 2 2, 7 3 2	部分署名計算部
1 1 3, 1 2 3, 1 3 3,	
3 1 3, 3 2 3, 3 3 3,	
5 1 3, 5 2 3, 5 3 3,	
7 1 3, 7 2 3, 7 3 3	部分署名署名化部
1 1 4, 1 2 4, 1 3 4,	
3 1 4, 3 2 4, 3 3 4,	
5 1 4, 5 2 4, 5 3 4,	
7 1 4, 7 2 4, 7 3 4	公開鍵暗号計算部
1 1 5, 1 2 5, 1 3 5,	
3 1 5, 3 2 5, 3 3 5,	
5 1 5, 5 2 5, 5 3 5,	
7 1 5, 7 2 5, 7 3 5	秘密鍵
1 1 6, 1 2 6, 1 3 6,	
3 1 6, 3 2 6, 3 3 6,	
5 1 6, 5 2 6, 5 3 6,	
7 1 6, 7 2 6, 7 3 6	データ記憶部
1 4 0, 3 4 0, 5 4 0, 7 4 0	移動エージェント
1 4 1, 3 4 1, 5 4 1, 7 4 1	中間データ格納部

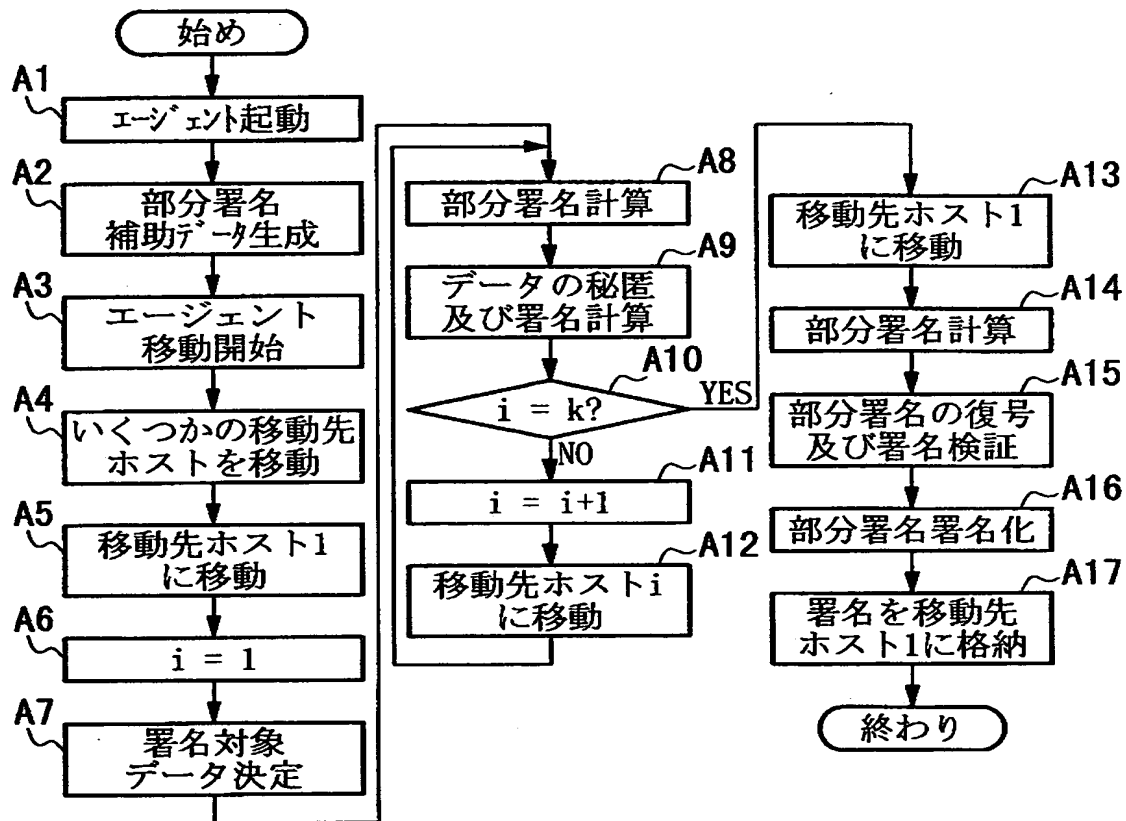
【書類名】

図面

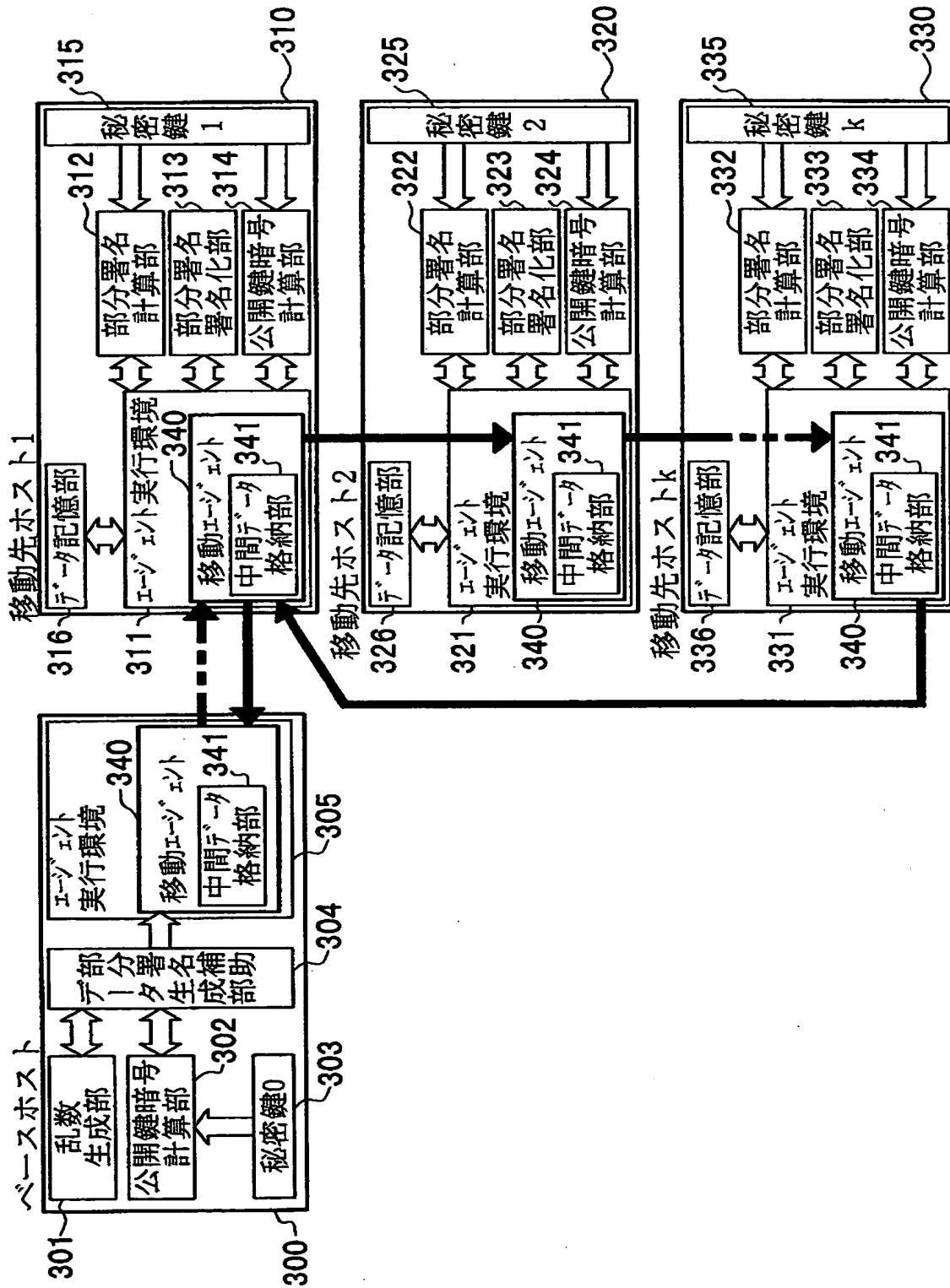
【図 1】



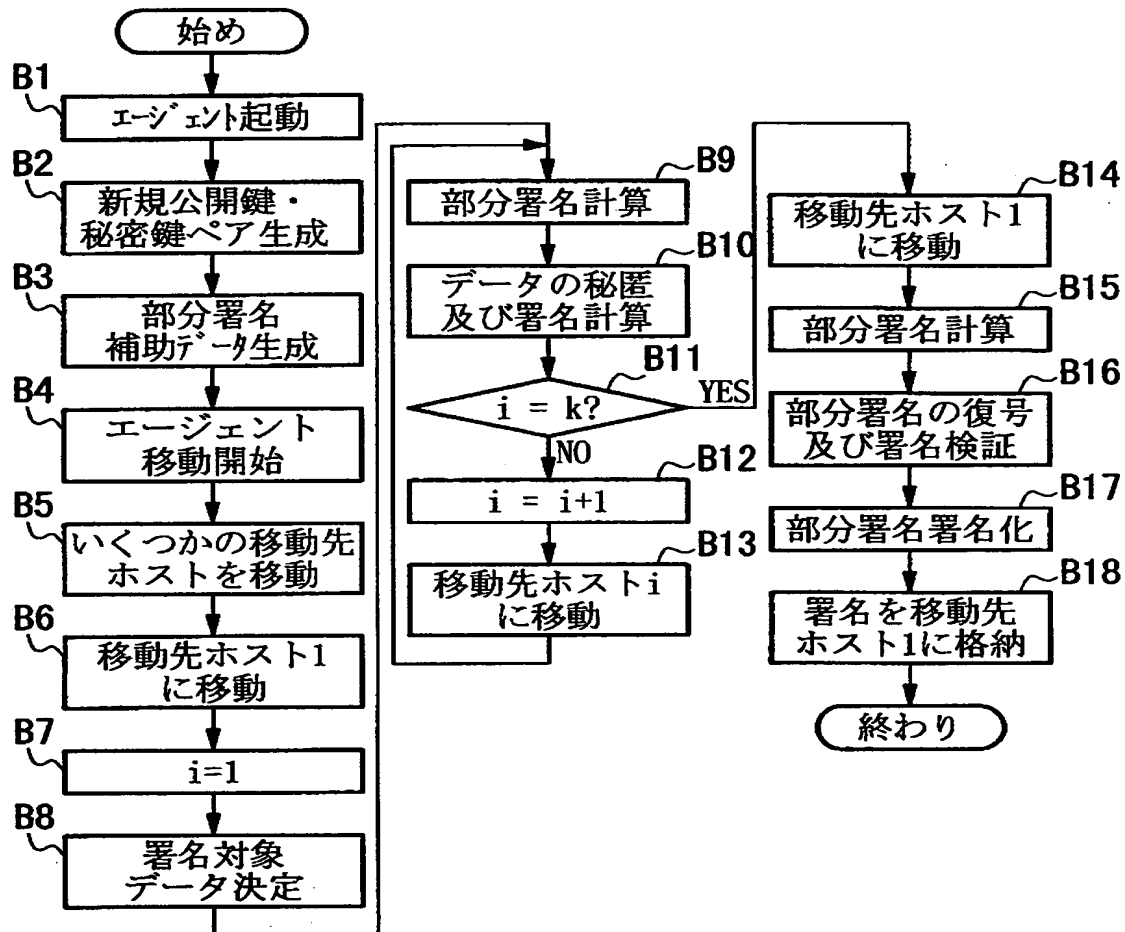
【図2】



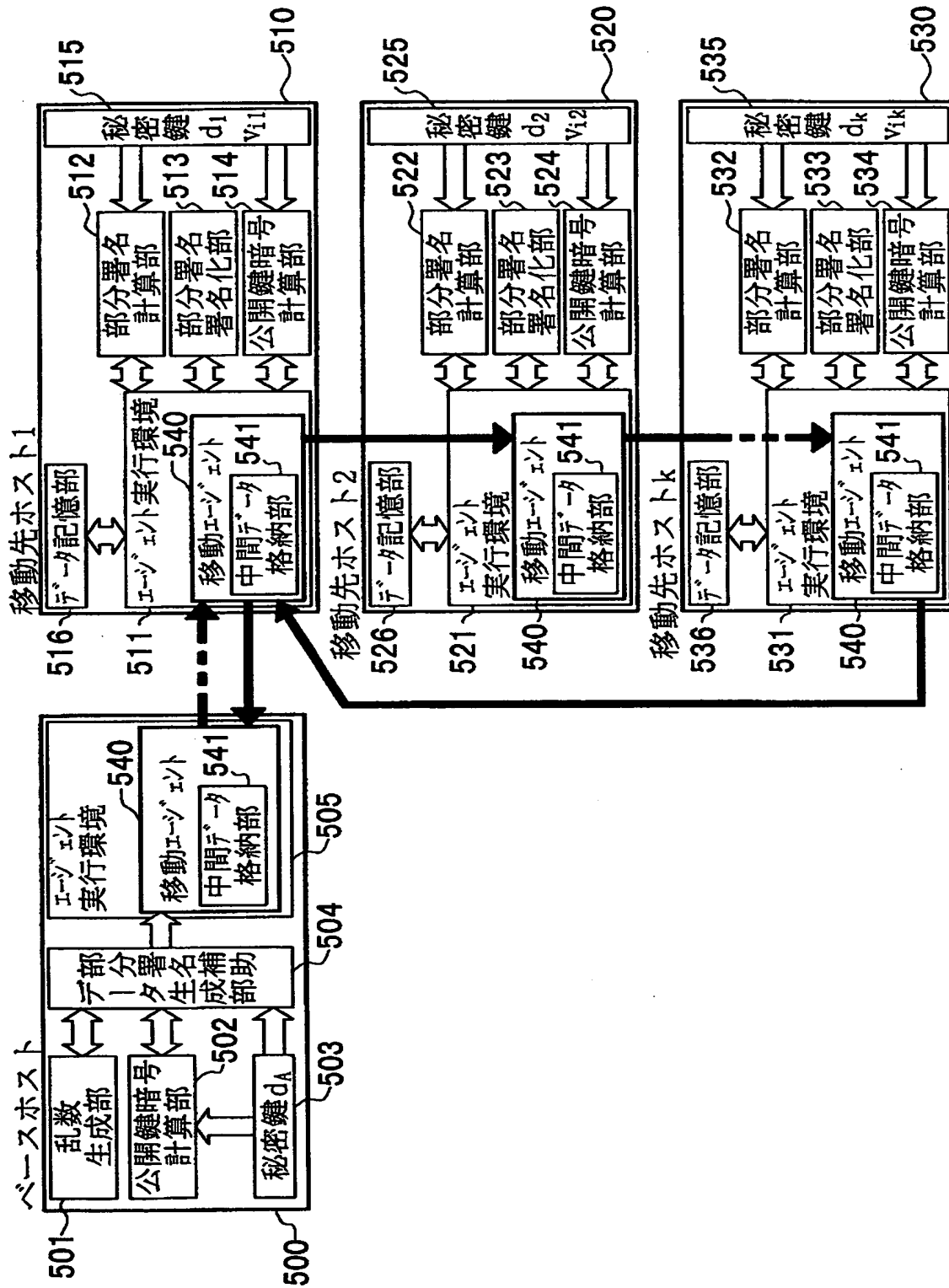
【図 3】



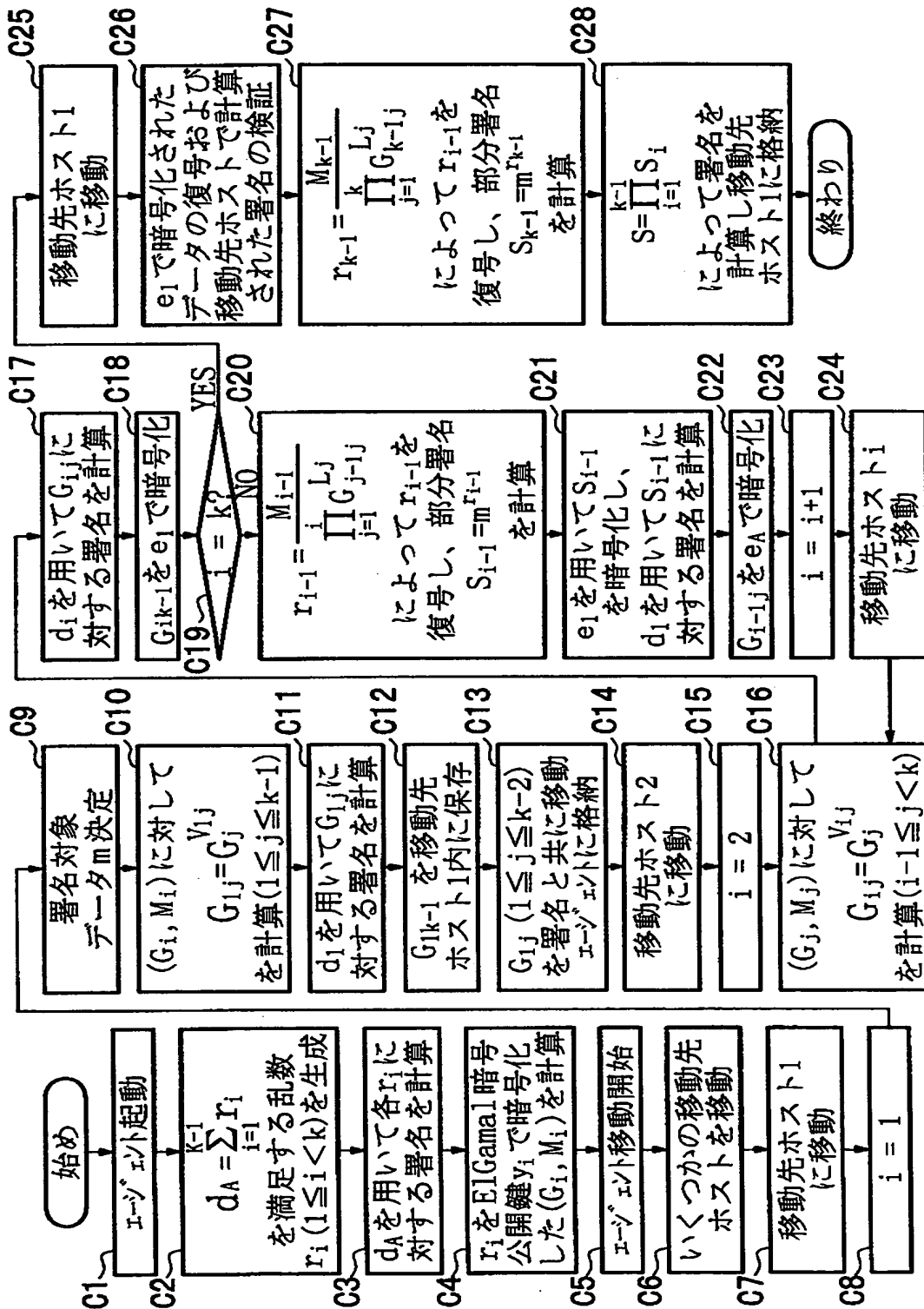
【図4】



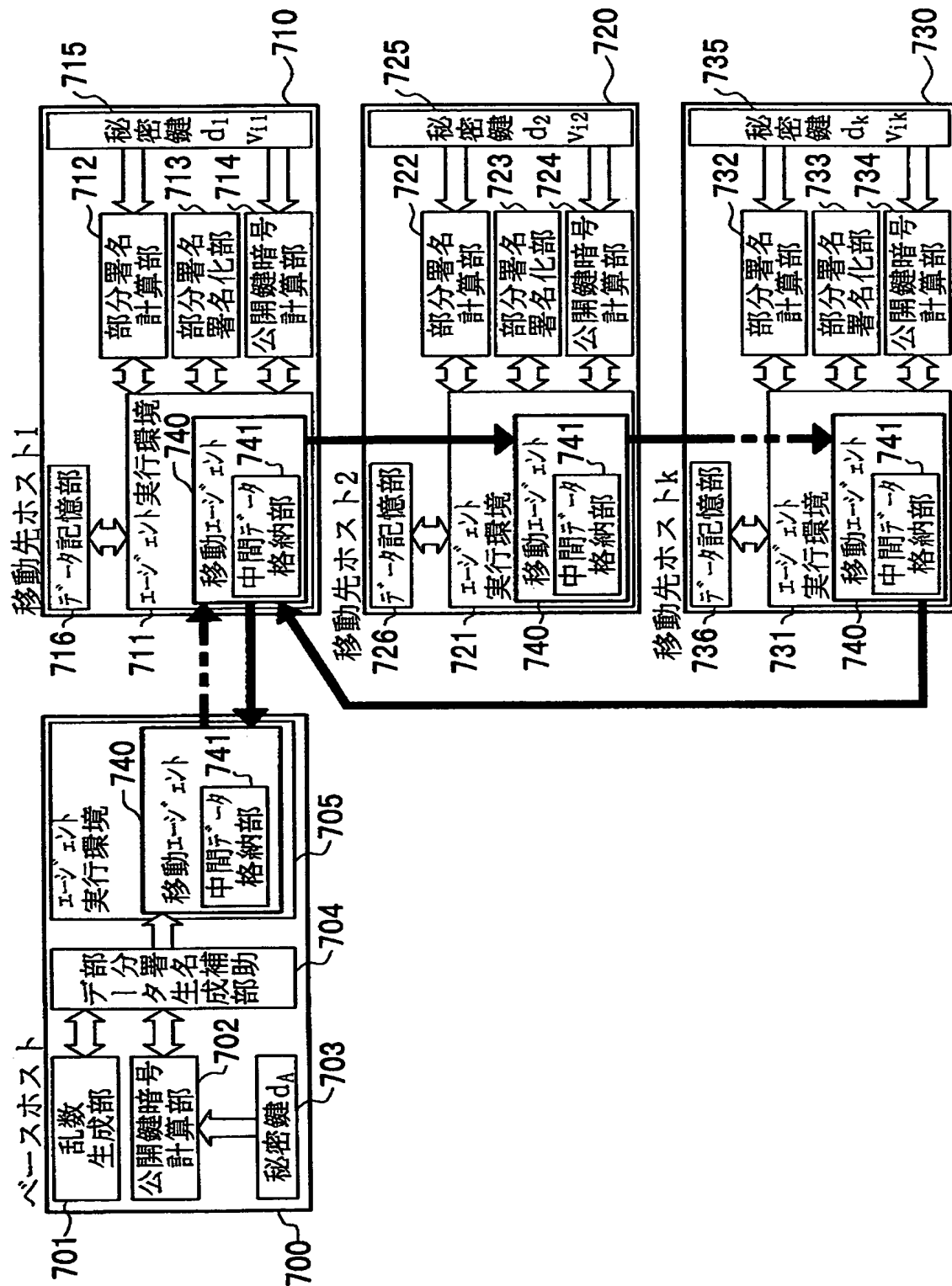
【図5】



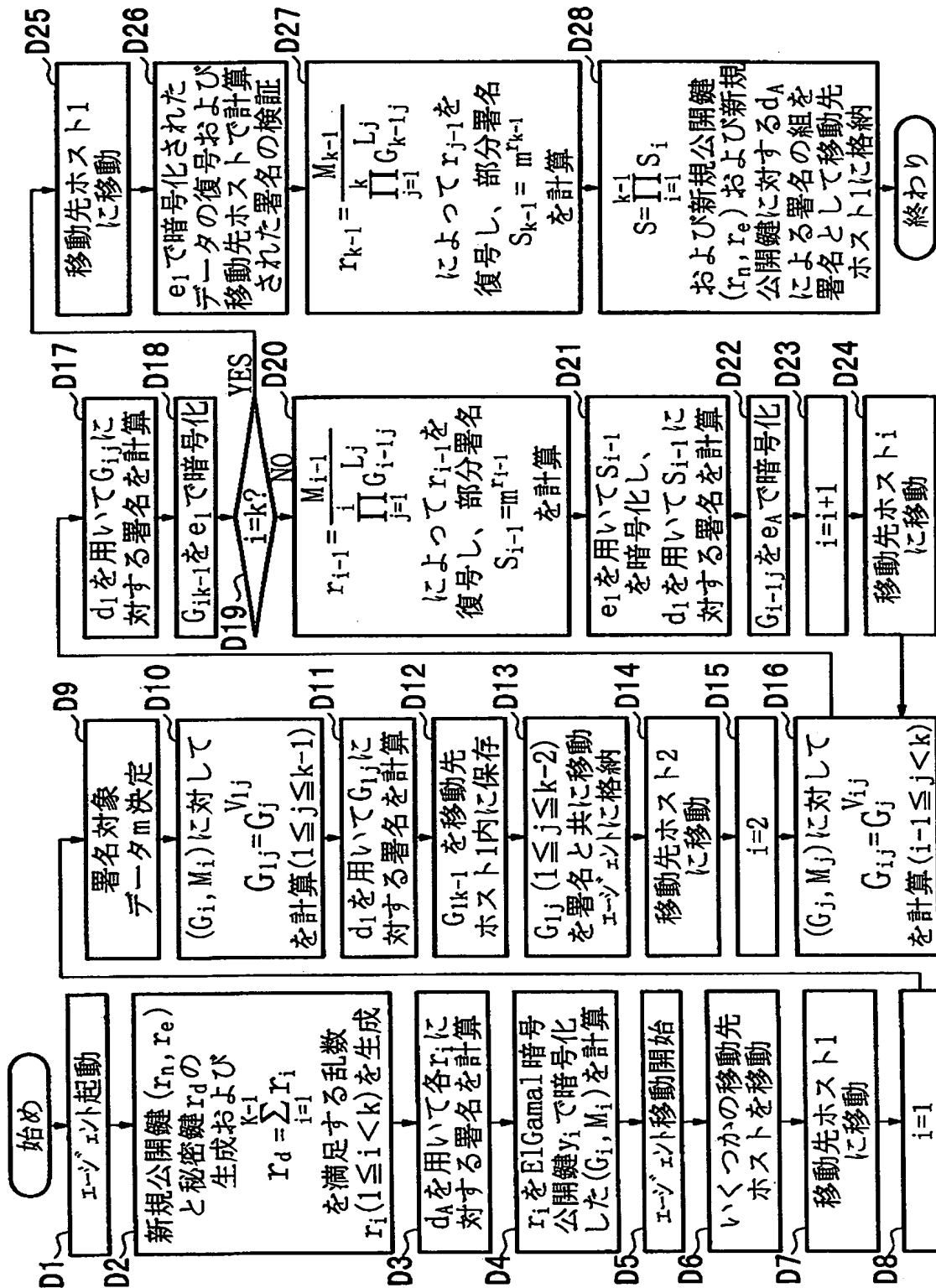
【図 6】



【図7】



【図 8】



【書類名】 要約書

【要約】

【課題】 プログラム・コードおよびデータを解析されても、移動先のホストに署名を偽造されない形で移動エージェントにデータを保持させ、移動先のホストで提示された任意のデータに対してデジタル署名を計算させるようにする。

【解決手段】 移動エージェント140が起動されるベースホスト100において、移動エージェントの所有者の秘密鍵0（103）を、部分署名補助データ生成部104によってk個の移動先ホスト110、120、130の秘密鍵115、125、135を用いた演算を行うことではじめて復元可能となるような形態に分割する。移動エージェントが訪れる各移動先ホストは、移動エージェントに格納されたデータと移動先ホストの秘密鍵とを部分署名計算部112、122、132への入力として部分署名を計算し、k個のホストが計算した部分署名から部分署名署名化部113、123、133を用いて実際の署名を得る。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2000-009037
受付番号	50000044624
書類名	特許願
担当官	高田 良彦 2319
作成日	平成12年 1月24日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000004237
【住所又は居所】	東京都港区芝五丁目7番1号
【氏名又は名称】	日本電気株式会社

【代理人】

申請人	
【識別番号】	100108578
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所
【氏名又は名称】	高橋 詔男

【代理人】

【識別番号】	100064908
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所
【氏名又は名称】	志賀 正武

【選任した代理人】

【識別番号】	100101465
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所
【氏名又は名称】	青山 正和

【選任した代理人】

【識別番号】	100108453
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所
【氏名又は名称】	村山 靖彦

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都港区芝五丁目7番1号

氏 名 日本電気株式会社

特許庁 登録部
特許出願第2000-009037号
出願日 1990年8月29日
出願人 日本電気株式会社